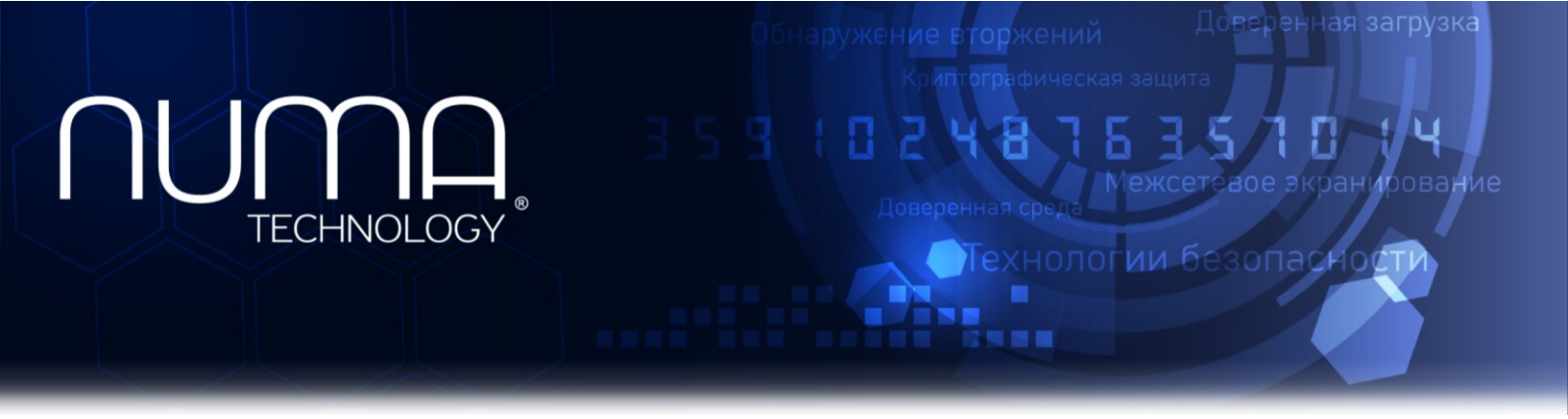

Средство доверенной загрузки уровня базовой системы ввода-вывода

Модуль доверенной загрузки Numa Arce

Руководство администратора

643.АМБН.00002-01 32 01

Листов 113

2022

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Идентификация документа

Название документа	Руководство администратора
Обозначение документа	643.АМБН.00002-01 32 01
Версия документа	1.1.1
Тип Изделия	Средство доверенной загрузки уровня базовой системы ввода-вывода 4 класса
Идентификация Изделия	Модуль доверенной загрузки Numa Arce
Идентификация требований	«Требования к средствам доверенной загрузки», утвержденные приказом ФСТЭК России от 27 сентября 2013 г. № 119. «Профиль защиты средств доверенной загрузки уровня базовой системы ввода-вывода четвертого класса защиты ИТ.СДЗ.УБ4.ПЗ» (ФСТЭК России, 2013); «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденного приказом ФСТЭК России от 02 июня 2020 г. № 76 по 4 уровню доверия. Задание по безопасности 643.АМБН.00002-01 47 01
Идентификация разработчика	ООО «НумаТех»
Ключевые слова	СДЗ, средство доверенной загрузки уровня базовой системы ввода-вывода

1.2. Аннотация

Данное руководство предназначено для администраторов Изделия модуль доверенной загрузки Numa Arce 643.АМБН.00002-01 (далее – Изделие или Numa Arce).

Руководство содержит все необходимые сведения, необходимые для установки, настройки, эксплуатации Изделия.

Перед началом работы с Изделием администратор должен ознакомиться с настоящим руководством.

2. ОБЩИЕ СВЕДЕНИЯ

2.1. Назначение

Изделие предназначено для выполнения доверенной загрузки, заключающейся в осуществлении запуска с доверенных и предопределенных заранее носителей только проверенного набора данных, проверки аппаратных ресурсов, идентификации и аутентификации пользователей, разграничения доступа на основе ролей, а также организации доверенной загрузки ОС после процедуры контроля целостности загружаемой среды.

2.2. Функциональные возможности Изделия

Изделие обеспечивает выполнение следующих функциональных возможностей

– возможность генерации и регистрации возникновения событий, относящихся к безопасности и контролируемых средством доверенной загрузки;

– возможность реагирования на обнаружение событий, указывающих на возможное нарушение безопасности;

– возможность блокирования пользователя на период, установленный администратором (от 3 до 60 минут) при превышении установленного администратором количества (от 1 до 8) неуспешных попыток аутентификации пользователя;

– возможность проверки соответствия аутентификационной информации определенной метрике качества (алфавит пароля 75 символов, длин пароля от 1 до 20 символов);

– возможность установления ограничений на время действия аутентификационной информации (пароля) на срок от 30 до 365 дней, вводимой (вводимого) пользователем в диалоговом интерфейсе при идентификации/аутентификации и блокирования доступа пользователя при превышении ограничений идентификация и аутентификация пользователя до выполнения действий по загрузке полезной нагрузки или администратора до выполнения действий по управлению средством доверенной загрузки;

– возможность идентификации и аутентификации с помощью логина и пароля или носителя ключевой информации или при совместном использовании носителя ключевой информации и пароля;

– исключение отображения действительного значения аутентификационной информации при ее вводе пользователем в диалоговом интерфейсе путем отображения условных знаков типа «*»;

– возможность контроля целостности загружаемой полезной нагрузки (данных MBR, ОС), файлов, поставленных на контроль администратором Изделия (в том числе журнала транзакций Ext3/Ext4/NTFS, реестра Windows), конфигурационных параметров, ПО региона ME, GbE микросхемы путем вычисления контрольных сумм;

– возможность контроля целостности модулей БСВВ Numa BIOS, образа Изделия, полезной нагрузки, загружаемой с помощью HTTP Boot путем проверки валидности и верифицированности цифровой подписи;

– возможность со стороны администраторов управлять режимом выполнения функций безопасности средства доверенной загрузки;

– возможность со стороны администраторов управлять данными (данными средства доверенной загрузки), используемыми функциями безопасности средства доверенной загрузки;

– поддержка определенных ролей (возможность создания учетных записи пользователей с ролями администратор, пользователь, аудитор) для средства доверенной

загрузки и их ассоциации с конкретными администраторами средства доверенной загрузки и пользователями информационной системы;

– возможность тестирования (самотестирования) функций безопасности средства доверенной загрузки, проверки целостности программного обеспечения средства доверенной загрузки и целостности данных средства доверенной загрузки;

– блокирование загрузки операционной системы при выявлении попыток загрузки нештатной операционной системы;

– реализация сценариев блокировки (по длительности блокировки) Изделия при превышении порога неуспешных попыток аутентификации пользователя;

– блокирование загрузки операционной системы при нарушении целостности средства доверенной загрузки;

– блокирование загрузки операционной системы при нарушении целостности загружаемой программной среды;

– блокирование загрузки операционной системы при критичных типах сбоев и ошибок;

– возможность контроля состава компонентов аппаратного обеспечения средства вычислительной техники, основываясь на их идентификационной информации;

– блокирование загрузки операционной системы при обнаружении несанкционированного изменения состава аппаратных компонентов;

– обеспечение недоступности информационного содержания ресурсов средств вычислительной техники, использовавшихся в процессе работы средства доверенной загрузки программным обеспечением и данными средства доверенной загрузки после завершения работы средства доверенной загрузки.

2.3. Роли пользователей, поддерживаемые Изделием

Изделие поддерживает три роли пользователей:

Администратор – пользователь, наделенный полными правами и привилегиями по настройке (администрированию) Изделием.

Пользователь – пользователь, наделенный правами по загрузке уже сконфигурированной полезной нагрузки (операционной системы).

Аудитор – администратор, наделенный правами по просмотру контроля целостности Изделия, файлов, поставленных на контроль администратором, а также имеющий возможность просмотр и выгрузку на USB-накопитель журнала аудита.

2.4. Режимы функционирования Изделия

Изделие поддерживает следующие режимы работы

2.4.1. Режим администрирования

Переход в режим администрирования осуществляется пользователем, наделенным полными правами и привилегиями по администрированию Изделия (далее – Администратор).

В режиме администрирования доступна настройка основных параметров и конфигураций Изделия.

2.4.2. Штатный режим функционирования Изделия

Переход в штатный режим работы осуществляется автоматически после идентификации и аутентификации пользователя, обладающего ролью пользователя, или администратора для загрузки ОС.

В штатном режиме работы предусмотрена только загрузка ОС и не предусмотрено выполнение никаких административных функций.

2.4.3. Режим работы для аудитора

После авторизации аудитора на экране Изделия появляется меню, которое состоит из профилей загрузки и пункта «Панель управления». В данном режиме аудитору доступно две функции:

– проверка и просмотр результатов контроля целостности Изделия, файлов и объектов, поставленных на контроль администратором Изделия;

– действия с журналом аудита: просмотр, экспорт на USB-носитель.

2.4.4. Аварийный режим

При аварийном режиме работы Изделия предусматривается блокировка СВТ, на которое установлено Изделие в связи с нарушением контроля целостности Изделия или среды функционирования. Дальнейшая работ Изделия возможна только после переустановки Изделия в режиме начальной инициализации.

2.4.5. Режим начальной инициализации

Режим начальной инициализации доступен только при первом запуске Изделия, или при восстановлении из-за нарушения контроля целостности Изделия. При режиме инициализации все установленные администратором данные стираются, Изделие возвращается к заводским настройкам.

2.5. Требования по безопасной приемке Изделия

При получении Изделия заказчик должен:

– обследовать поставку на предмет полноты комплектности и отсутствия механических повреждений. Комплект поставки должен состоять из частей, описанных в Формуляре 643.АМБН.00002-01 30 01;

– убедиться, что в Формуляре заполнены все необходимые графы, стоят соответствующие печати и подписи, Формуляр Изделия промаркирован идентификатором СЗИ и номером экземпляра;

– убедиться, что компакт-диск расположен в конверте, заклеенном наклейкой с логотипом ООО «НумаТех», отсутствуют видимые признаки вскрытия конверта, а прописанные идентификатор СЗИ и номер экземпляра совпадают с теми, что прописаны в Формуляре на Изделие;

– ознакомиться с документацией на Изделие;

– перед эксплуатацией Изделия необходимо провести контроль целостности неизменных файлов Изделия согласно документу «Инструкция по проверке контрольных сумм» 643.АМБН.00002-01 94 01, входящему в комплект поставки.

ПРИМЕЧАНИЕ. Убедиться, что в документе «Сервисный сертификат», входящего в комплект поставки, имеются отметка о дате продажи, печать продавца и сведения об уполномоченном представителе продавца. Без данных отметок техническая поддержка и гарантийное обслуживание Изделия будут недоступны.

2.6. Дополнительные требования

Изделие может функционировать только в среде базовой системы-ввода-вывода Numa BIOS 643.АМБН.00001-01 производства ООО «НумаТех».

Для обновления Изделия требуется USB-накопитель с файловой системой FAT32.

Изделие поставляется в виде файла-прошивки, предназначенного для дальнейшего тиражирования и установки на СВТ.

При работе с технологией HTTP Boot генерацию ключей для цифровой подписи необходимо выполнять в доверенной ОС.

2.7. Требования безопасности

Должен быть обеспечен контроль целостности СВТ, на который установлено Изделие, а также контроль конфигурации аппаратного обеспечения СВТ.

При первоначальной настройке Изделия необходимо изменить заводские установки паролей на доступ к функциям администрирования Изделия.

Необходимо сохранение в секрете идентификаторов (имен) и паролей (кодов) администратора Изделия.

Обновление Изделия должно осуществляться только с использованием файла-прошивки, полученной от изготовителя, в т.ч. скачанной с его официального сайта, с соблюдением соответствующих Инструкций изготовителя.

Изменение версии Изделия на другую версию возможно только в том случае, если изготовителем подтверждено соответствие данной версии Изделия требованиям безопасности информации путем проведения анализа уязвимостей и периодических испытаний Изделия.

Изделие должно использоваться строго в соответствии с положениями, приведенными в данном руководстве.

Запрещается модифицировать, реконструировать или видоизменять Изделие.

Установка, конфигурирование и управление Изделием должны производиться только администратором в соответствии с данным руководством.

3. УСТАНОВКА И ЛИЦЕНЗИРОВАНИЕ ИЗДЕЛИЯ

Изделие может поставляться:

– в предустановленном на СВТ виде;

– в виде файла-прошивки готового к установке на СВТ.

3.1. Установка Изделия

В случае поставки Изделия в предустановленном на СВТ виде установка и активация Изделия осуществляется Изготовителем СВТ, на которое устанавливается Изделие. Идентификационная и аутентификационная информация (логин-пароль) администратора установленного Изделия должна быть получена от Изготовителя СВТ, на которое установлено Изделие.

В случае поставки Изделия в виде файла-прошивки необходимо произвести установку и активацию Изделия самостоятельно.

Установка и активация Изделия в СВТ, которое содержит в своем составе базовую систему ввода-вывода Numa BIOS, осуществляется путем активации файла-лицензии. Для этого необходимо сгенерировать файл-запрос лицензии:

– в главном меню БСВВ Numa BIOS перейти в раздел «Версия БСВВ»→ «Информация о лицензии»;

– подключить USB-накопитель в СВТ для сохранения файла-запроса лицензии;

– в меню «Информация о лицензии» выбрать пункт «Сохранить файл запроса»;

– убедиться, что Изделие выдало сообщение «Запрос лицензии успешно сохранен» и файл сохранился на USB-накопитель;

– передать сгенерированный файл-запрос в сервисную службу ООО «НумаТех» по электронному адресу, указанному в документе «Формуляр» 643.АМБН.00002-01 30 01;

– на основе файла запроса формируется файл-лицензия вида xxx.p12;

– полученный файл-лицензию необходимо перенести на USB-накопитель и подключить его к СВТ;

– перейти в меню «Версия БСВВ»→ «Информация о лицензии»;

– выбрать пункт «Загрузить файл лицензии» и в открывшемся браузере выбрать файл-лицензию;

– нажать клавишу «Enter» и убедиться, что появилось сообщение «Лицензия установлена!» после чего автоматически произойдет установка Изделия и автоматическая перезагрузка СВТ.

Изделие активируется на СВТ и запустится в режиме «Подготовка к работе» см. пункт 3.4.

Внимание! В процессе активации функций Модуля доверенной загрузки все данные и настроенные параметры будут возвращены к заводским настройкам.

Для установки Изделия на СВТ, которые **не** содержат в своем составе базовую систему ввода-вывода Numa BIOS необходимо:

Примечание*. Для установки Изделия требуется USB-накопитель с файловой системой FAT32.*

Внимание! Процедура безопасной установки Изделия должна начинаться с проверки контрольной суммы полученного Изделия на соответствие сертифицированной версии! Процедура выполняется согласно документу «Инструкция по проверке контрольных сумм» 643.АМБН.00002-01 94 01.

1) скопировать файловый архив, содержащий файл-прошивку с компакт-диска, входящего в комплект поставки, на USB-накопитель с файловой системой FAT32;

2) распаковать содержимое архива в корневую папку подготовленного USB-накопителя;

3) подключить подготовленный USB-накопитель с файлом-прошивкой к СВТ и произвести загрузку в EFI-режиме;

В автоматическом режиме после загрузки запустится скрипт перепрошивки штатного BIOS (см. рисунок 1);

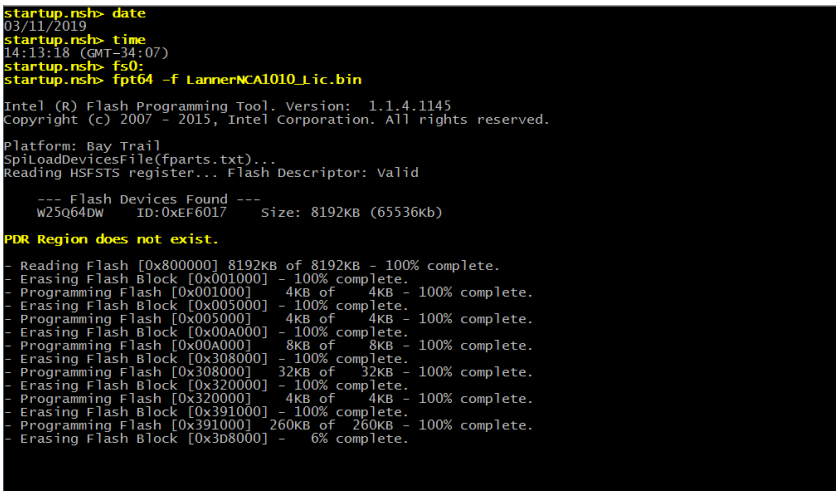

Рисунок 1 – Работа скрипта прошивки БСВВ

***Примечание**. В конце работы скрипта возможны сообщения об ошибках верификации, данные ошибки необходимо проигнорировать.*

4) после окончания работы скрипта необходимо нажать клавишу «Enter» для перезагрузки СВТ.

3.2. Запуск Изделия

Запуск и загрузка Изделия осуществляется автоматически после подачи электропитания на СВТ и нажатия кнопки «power» на СВТ.

Во время загрузки Изделия в консоль выводится логотип ООО «НумаТех», шкала хода загрузки.

3.3. Запрос и загрузка лицензии

После перезагрузки Изделия активизируется режим проверки лицензии на Изделие. Форма «ручной режим запроса лицензий» (см. рисунок 2) позволяет:

– «Сохранить файл запроса» – сохраняет файл с уникальным идентификатором на USB-носитель. Этот файл должен быть передан в сервисную службу ООО «НумаТех» по электронному адресу, указанному в документе «Формуляр» 643.АМБН.00002-01 30 01, для создания файла лицензии;

– «Загрузить файл лицензии» – загрузить полученный файл лицензии для

дальнейшей работы Изделия;

– «Перейти в OEM-режим» – режим, при котором доступна тестовая версия Изделия, максимальное количество попыток загрузки 10;

***Примечание**. В зависимости от типа СВТ пункт «Перейти в OEM-режим» может отсутствовать.*

– «Настройка даты и времени» – настройка системных часов.

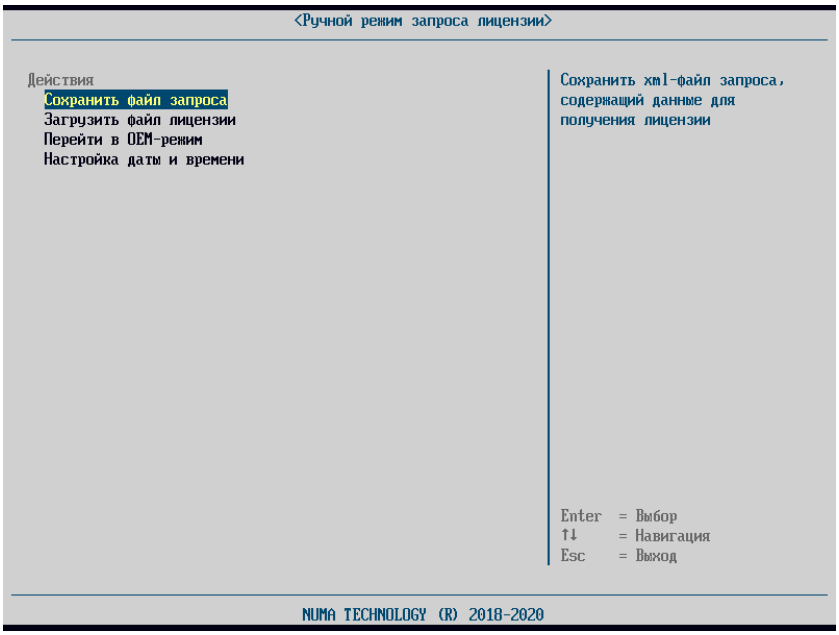

Рисунок 2 – Ручной режим запроса лицензии

Для создания файла запроса для получения лицензии необходимо в меню «Ручной ввод лицензии» необходимо выбрать пункт «Сохранить файл запроса». Необходимые данные будут сохранены на USB-накопитель в файл с именем «numa_license_req_XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX.xml».

Созданный файл необходимо отправить в сервисную службу ООО «НумаТех» для получения файла лицензии.

На основе файла запроса лицензии будет создан файл лицензии («XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX.p12»).

Для активации лицензии необходимо полученный файл лицензии загрузить через пункт меню «Загрузить файл лицензии». После проверки лицензии работа Изделия будет разблокирована, Изделие будет доступно для дальнейшей настройки и использования после перезагрузки СВТ.

***Примечание**. При подключении USB-носителя в СВТ Изделие автоматически проверит наличие лицензии в каталоге bios и предложит ее к загрузке при наличии. В случае отсутствия лицензии в каталоге bios необходимо выбрать лицензию на подключенном USB-накопителе вручную.*

В случае если выбран файл от неверной платформы, появляется сообщение об ошибке – «Проверка лицензии завершилась с ошибкой!». В этом случае необходимо проверить соответствие устанавливаемого файла с техническими характеристиками устройства, на которое производится установка. При появлении ошибки повторно следует

обратиться в службу технической поддержки Изготовителя СВТ, на которое устанавливается Изделие, или сервисную службу компании ООО «НумаТех» по электронной почте, указанной в документе «Формуляр» 643.АМБН.00002-01 30 01.

3.4. Подготовка к работе

При первом включении Изделия в консоль могут выводиться сообщения об ошибках «DebugAssert...», ошибки такого типа следует игнорировать.

При первом включении Изделия необходимо создать учётную запись администратора.

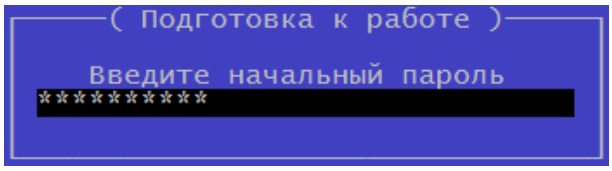

Рисунок 3 – Диалог ввода пароля для меню «Подготовка к работе»

Для этого в режиме «Подготовка к работе» (см. рисунок 3) необходимо ввести начальный пароль «**capitolium**» для дальнейшей первоначальной настройки Изделия.

После ввода пароля будет доступно меню (см. рисунок 4), состоящее из пунктов:

– «Создать Администратора» – создание учетной записи администратора СВТ;

– «Загрузить с USB» – загрузка подготовленного списка пользователей, включая администратора;

– «Дата и время» – настройка системных часов;

– «Сертификаты» (см. п. 5.7.2 «Сертификаты»);

– «Управление токеном» – инициализация токена при первом подключении (см. п. 5.7.1.5 «Управление токеном»)

Для дальнейшей работы необходимо создать учетную запись администратора. Для этого в меню, представленном на рисунке 4, выбрать раздел «Создать администратора». В форму, представленную на рисунке 5, необходимо ввести параметры администратора. После создания администратора вход в меню администрирования Изделия будет осуществляться с его учетными данными.

После успешного создания администратора следует перезагрузка Изделия.

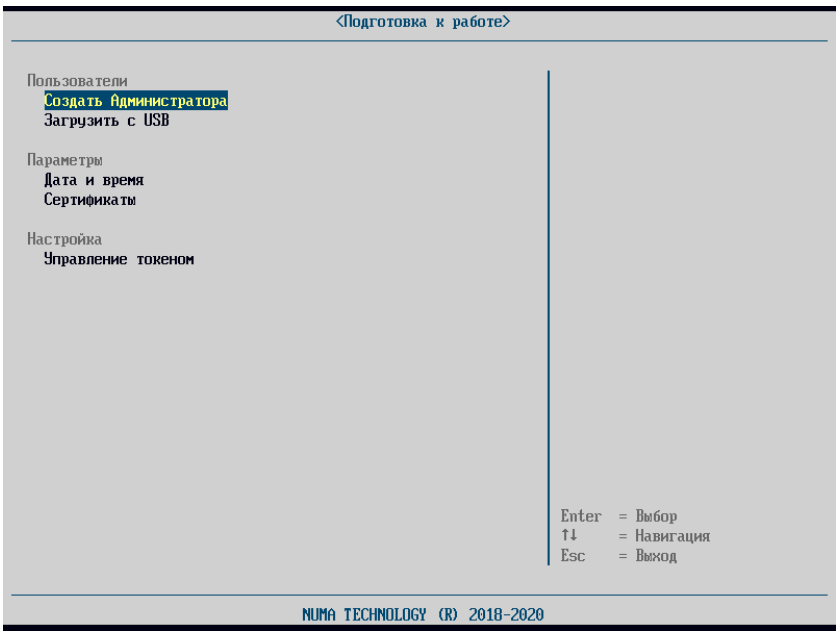

Рисунок 4 – Меню режима «Подготовка к работе»

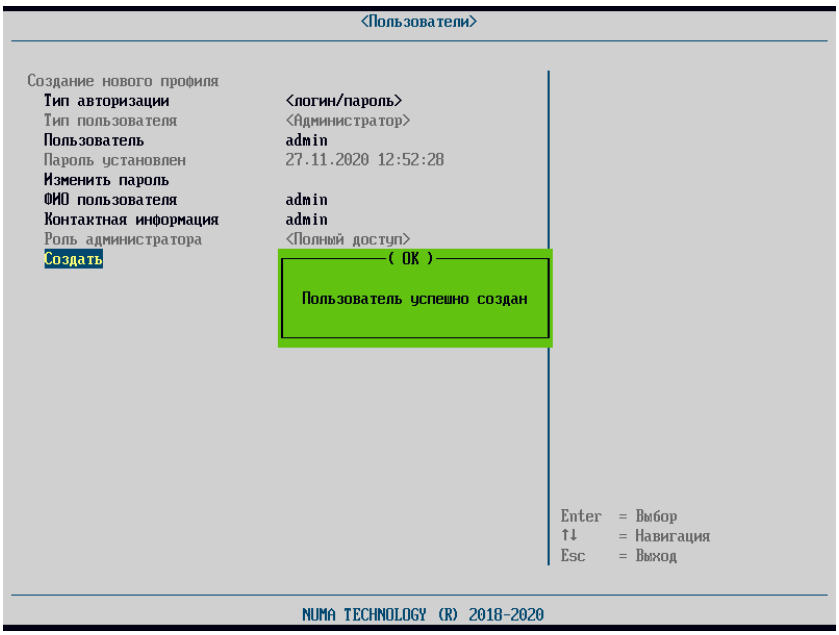

Рисунок 5 – Меню «Создать администратора»

Загрузка ОС СВТ из режима Подготовки к работе Изделия не предусмотрена.

3.5. Режим производства

После ввода лицензии и перезагрузки СВТ будет осуществлён автоматический вход в режим производства.

В данном режиме в главном меню доступны дополнительные пункты (см. рисунок 6):

– загрузить настройки БСВВ;

– сохранить настройки БСВВ;

– выход из режима производства.

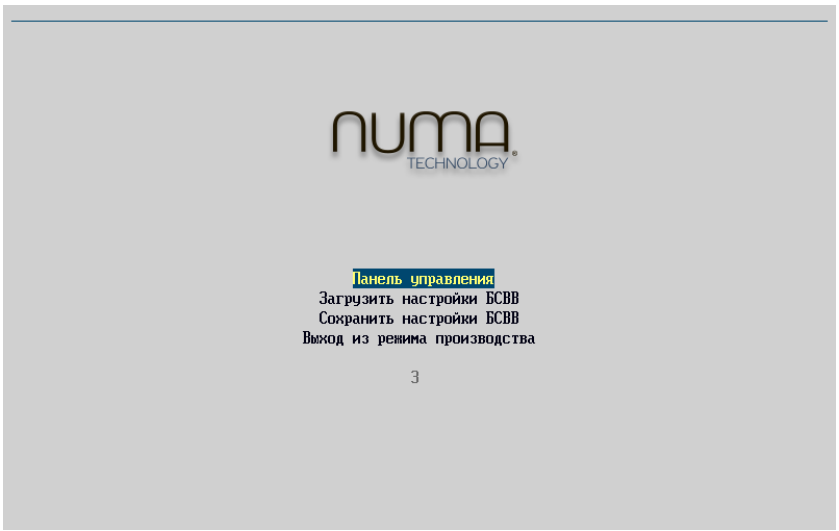

Рисунок 6 – Главное меню «Режима производства»

Выход из режима производства производится вручную – через пункт меню.

3.5.1. Создание файла настроек

Для создания файла настроек необходимо выполнить следующие действия:

– войти в меню «Панель управления»;

– внести необходимые изменения в настройки, например, создать загрузочный профиль, список пользователей и настройки портов SATA/USB;

– перезагрузиться (выход из панели управления в главное меню невозможен);

– выполнить пункт «Сохранить настройки БСВВ» – файл настроек будет сохранен на USB-накопитель в папку \bios;

– выйти из режима производства через соответствующий пункт меню;

3.5.2. Применение файла настроек:

Для применения файла-настроек необходимо выполнить следующие действия:

– установить USB-накопитель с сохраненным файлом настроек и включить изделие;

– если файл настроек существует, автоматически будет предложено загрузить его (см. рисунок 7);

– в случае согласия файл будет загружен и будет осуществлен автоматический выход из режима производства;

– в случае отказа пользователю предоставляется возможность выбрать файл вручную, выбрав пункт «Загрузить настройки БСВВ».

Выход из режима производства также производится вручную – через пункт меню.

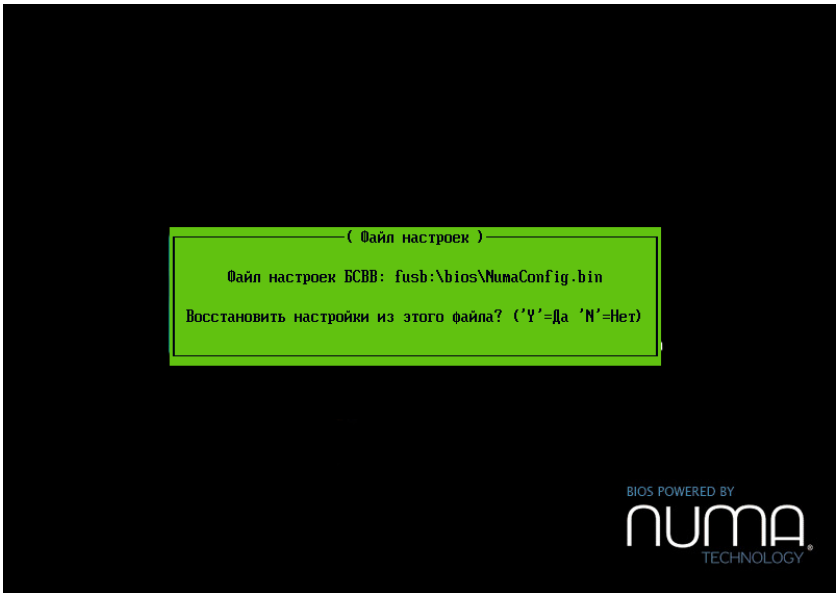

Рисунок 7 – Установка файла настроек

4. ОПИСАНИЕ ПРОЦЕДУР ПРОВЕРКИ ЦЕЛОСТНОСТИ

Изделие осуществляет проверку целостности всех компонентов, поставленных на контроль автоматически при каждом включении СВТ, также автоматически при входе в пункт меню администрирования «Контроль целостности».

4.1. Автоматический контроль целостности

После подачи питания на СВТ Изделие автоматически осуществляется контроль целостности следующих компонент с вычислением контрольной суммы по ГОСТ Р 34.11-2012-256 бит:

– файлы, поставленные на контроль администратором;

– данные MBR и ОС, поставленные на контроль администратором (в том числе реестр Windows, журнал транзакций Ext3/Ext4/NTFS);

– конфигурационные данные;

– программное обеспечение регионов ME, GbE микросхемы SPI flash.

Изделие обеспечивает контроль целостности по ГОСТ Р 34.10-2012 модулей БСВВ Numa BIOS, а также образа Изделия (Numa_Arce.efi).

В случае нарушения контроля целостности образа Изделия (ПО Изделия), модулей БСВВ Numa BIOS Изделие осуществляет переход в аварийный режим работы, который сопровождается сообщением об ошибке и блокировкой загрузки СВТ.

В случае нарушения контроля целостности локальных файлов MBR и ОС, файлов, поставленных на контроль администратором Изделия (объекты загружаемой операционной системы), ПО регионов ME, GbE осуществляется блокировка работы СВТ, выдача сообщения об ошибке, звуковой сигнал (только при наличии технической возможности), запись в журнал аудита.

> ***Примечание.*** *Дальнейшая блокировка требует снятие блокировки администратором Изделия путем перерасчета контрольных сумм.*

В случае нарушения контроля целостности конфигурационных параметров осуществляется блокировка загрузки СВТ, выдача сообщения об ошибке и предложение сохранить отладочный дамп для дальнейшего расследования инцидента. Изделие переходит в режим начальной конфигурации.

4.2. Проверка целостности вручную

Функция проверки целостности вручную предназначена для запуска принудительного контроля целостности бинарного образа Изделия, загружаемых компонент операционной среды, данных, поставленный на контроль, конфигурационных параметров при переходе в меню «Контроль целостности».

Для запуска проверки необходимо выполнить следующие действия:

– авторизоваться под учётной записью Администратора;

– зайти в меню «Панель управления»;

– выбрать пункт основного меню «Проверка целостности».

На экран будет выведена форма с результатами проверки всех компонентов (см. рисунок 8)

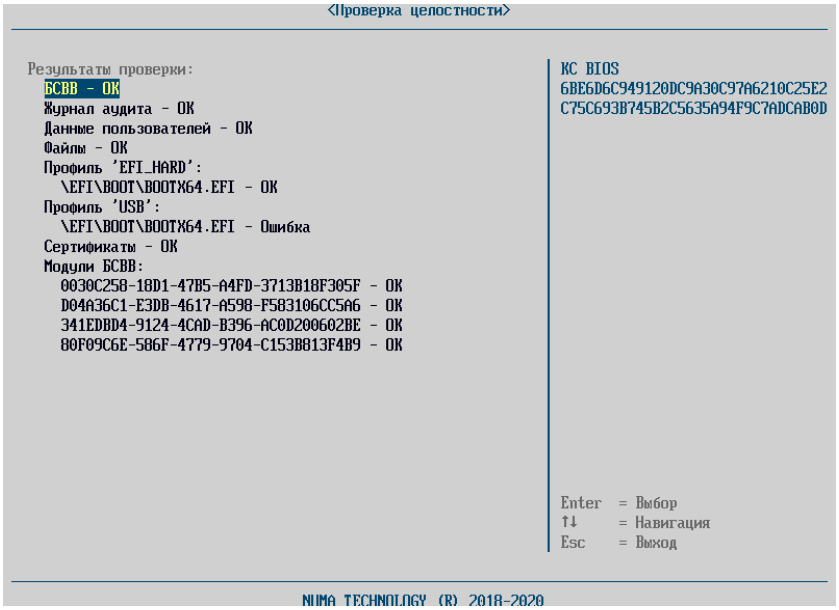

Рисунок 8 – Результат контроля целостности вручную

При наведении клавишами «↓» и «↑» выделения на одну из строк с объектами контроля целостности в правой части окна синим шрифтом отображается контрольная сумма этого объекта.

Управление списком файлов, для которых осуществляется контроль целостности, доступно из раздела «Редактирование профиля» пункта «Конфигуратор» меню «Панель управления» (см. п. 5.5.2.6).

5. ПРОЦЕДУРЫ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ О ПОЛЬЗОВАТЕЛЯХ И РЕЖИМЫ РАБОТЫ NUMA ARCE

5.1. Авторизация

После загрузки Изделия в штатном режиме работы появляется окно с приглашением выбрать тип авторизации пользователя (см. рисунок 9):

– по имени пользователя;

– с помощью АНП;

– с помощью АНП и логин/пароля.

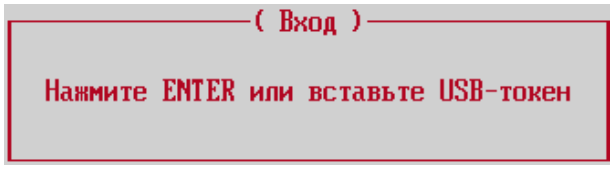

Рисунок 9 – Внешний вид окна с приглашением для выбора типа авторизации

Чтобы авторизоваться по имени пользователя (с помощью логина и пароля), необходимо выполнить следующие действия:

– после появления окна с приглашением к авторизации, нажать «Enter»;

– в окне «Пользователь» (см. рисунок 10) ввести имя пользователя;

Примечание. *Изделие не чувствительно к регистру вводимых символов имени пользователя (логина). Например, Admin, admin и AdMiN являются равнозначными.*

– в появившемся окне «Пароль» (см. рисунок 11) ввести пароль и нажать «Enter».

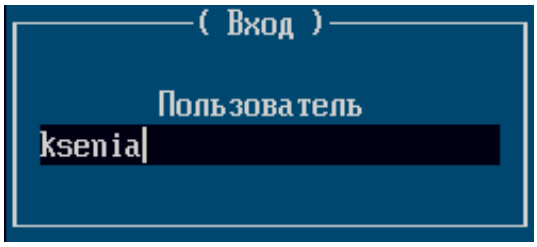

Рисунок 10 – Внешний вид авторизационного окна «Пользователь»

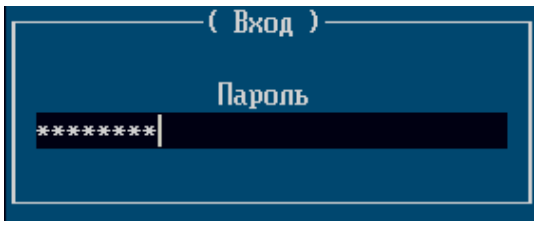

Рисунок 11 – Внешний вид авторизационного окна «Пароль»

Чтобы авторизоваться с помощью АНП, необходимо выполнить следующие действия:

– после появления окна с приглашением к авторизации, вставить АНП (далее – токен) в USB–разъем СВТ;

– ввести ПИН–код в соответствующем окне ввода и нажать «Enter».

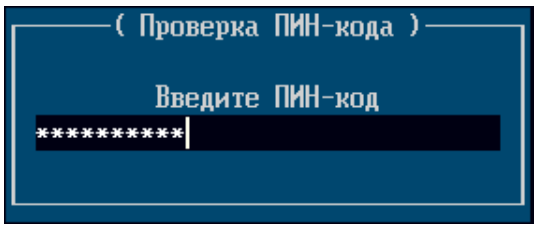

Рисунок 12 – Внешний вид окна при авторизации с помощью АПН

Если задан тип авторизации «АНП + логин/пароль», необходимо выполнить следующие действия:

– после появления окна с приглашением к авторизации, вставить токен в USB–разъем СВТ;

– ввести ПИН–код в соответствующем окне ввода и нажать «Enter»;

– в появившемся окне «Пользователь» ввести имя пользователя;

– в появившемся окне «Пароль» ввести пароль и нажать «Enter».

При вводе пароля или ПИН–кода вводимые символы отображаются на экране символами «*», количество которых равно числу введенных символов.

***Примечание**. В случае если предварительно в Изделие не был загружен сертификат, при попытке авторизации об этом будет выведено сообщение «СА не загружен!». После извлечения токена или нажатия клавиши «Enter» в этом случае пользователю в доступе будет отказано с выводом сообщения «Ошибка! Доступ запрещен!».*

***Примечание**. Количество попыток ввода ПИН-кода для токена ограничивается администратором организации при инициализации токена.*

В Изделии реализован механизм блокирования работы пользователи при превышении установленных администратором Изделия параметров. По умолчанию в Изделии установлены следующие параметры для защиты от несанкционированного доступа:

– количество неуспешных попыток ввода пароля – 3;

– время блокировки пользователи при превышении установленного количества неуспешных попыток ввода пароля – 15 минут.

Подробная информация о способах настройки парольной политики описана в разделе 5.7.1.4.

В Изделии также реализован механизм защиты от подбора логина. В случае если в форме идентификации введен неверный логин, а также введен пароль, то Изделие отобразит ошибку «Введен неверный пароль или логин», учетная запись заблокируется на 10 секунд, в форме отобразится таймер блокировки, осуществится запись в журнале аудита. При второй попытке учетная запись заблокируется на 30 секунд, при третьей и следующих попытках время блокировки с каждым разом будет увеличиваться на 30 секунд до достижения максимального количества попыток входа в систему, установленного администратором в парольной политике (см. раздел 5.7.1.4).

Любые действия по администрированию Изделием доступны только после успешной процедуры авторизации.

5.2. Авторизация пользователя с использованием сервера LDAP

Для настройки возможности авторизации пользователя с помощью сервера LDAP необходимо выполнить следующие действия:

– настроить сетевую карту:

– выбрать пункт меню «Драйверы устройств» → «ETH0: настройка IPv4»;

– включить чекбокс ([X]) «Использовать IPv4» – станут доступны пункты меню для редактирования сетевых настроек;

– задать необходимые значения параметров сетевой карты при использовании статических настроек (IP–адрес, маску подсети и IP-адрес шлюза по умолчанию) или включить флаг «Включить DHCP» при использовании динамических настроек сетевой карты;

– сохранить настройки с помощью клавиши F10;

– настроить клиент LDAP (см. Рисунок 13):

а) включить опцию «Использовать авторизацию LDAP» в меню «Дополнительно» → «Настройка авторизации LDAP»;

б) задать необходимые настройки:

1) «IP-адрес» и/или «Имя сервера LDAP» в случае, если не используется DNS;
2) «Номер порта сервера LDAP»;
3) «Домен» (название домена, в котором будет происходить поиск пользователей);
4) «Рабочие станции» (название узла сервера LDAP, в котором расположены рабочие станции);
5) «DN администратора» (полное имя пользователя на сервере LDAP, обладающего правом на поиск авторизуемых пользователей на сервере LDAP и запрос их DN с сервера. Связка «DN авторизуемого пользователя» и «Пароль» используется для авторизации);
6) пароль;
7) «Использовать TLS» (флаг–признак использования TLS);

– сохранить изменения;

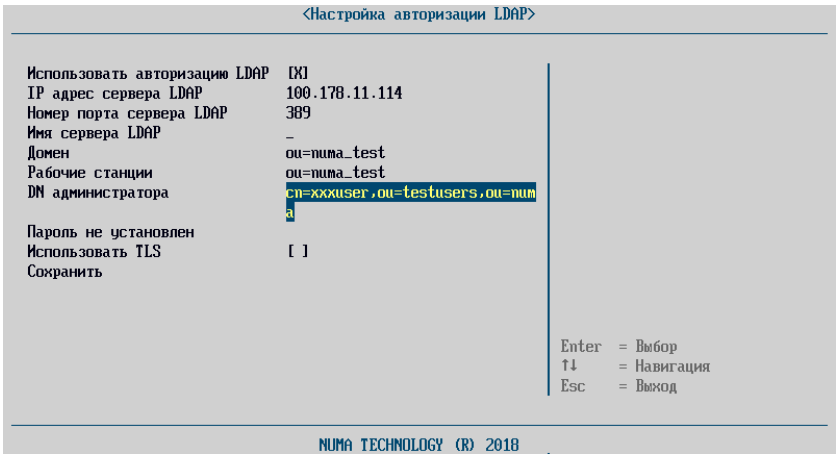

Рисунок 13 – Настройки авторизации LDAP

– настроить AD LDS для работы с Изделием и синхронизации с основным AD согласно руководству 643.АМБН.00002-01 93 01 (предоставляется по требованию).

5.3. Главное меню

После успешной авторизации администратора или аудитора на экране отображается меню, которое содержит список профилей загрузки (при условии, что профили были созданы

заранее) и пункт «Панель управления» (см. рисунок 14).

В случае успешной авторизации пользователя произойдет автоматическая загрузка профиля загрузки, если настроенный администратором профиль единственный, или отобразится главное меню со всеми доступными профилями загрузки. Пункт «Панель управления» для пользователя не предусмотрен.

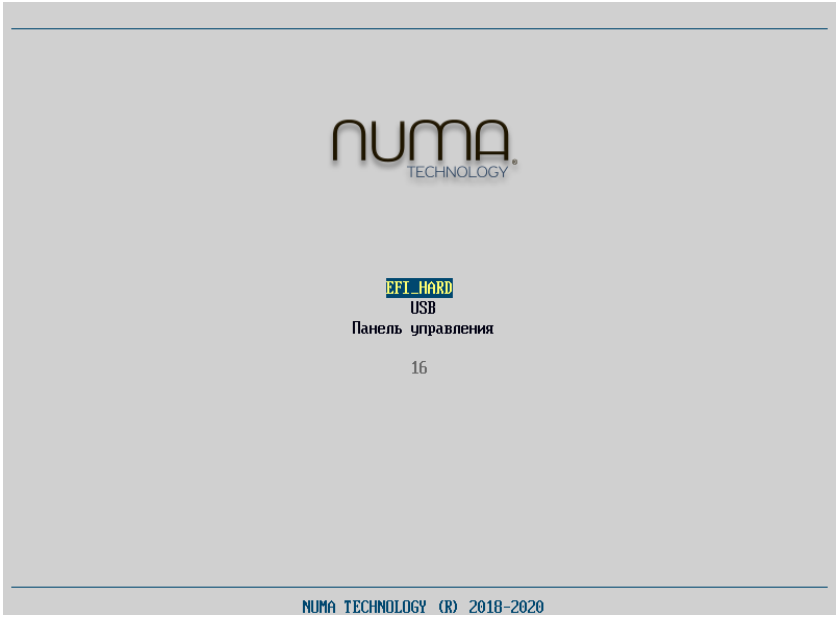

Рисунок 14 – Главное меню

По умолчанию меню на экране отображается в течение 7 сек., после чего происходит запуск профиля загрузки СВТ, если он один, или первого из списка профилей, если их более одного. Если была нажата какая-либо клавиша, меню будет отображаться на экране вплоть до выбора соответствующего пункта.

Настроить тайм-аут можно в пункте меню «Конфигуратор».

Переход и выбор пунктов меню осуществляется за счет клавиш навигации: «↑», «↓», «Enter».

5.4. Меню «Панель управления»

«Панель управления» является оснасткой для администрирования Изделием и позволяет выбрать носитель для загрузки ОС, создать конфигурацию загрузки и настроить параметры Изделия.

В панели управления администратору с полным доступом доступно 17 пунктов меню, сгруппированных в 4 раздела.

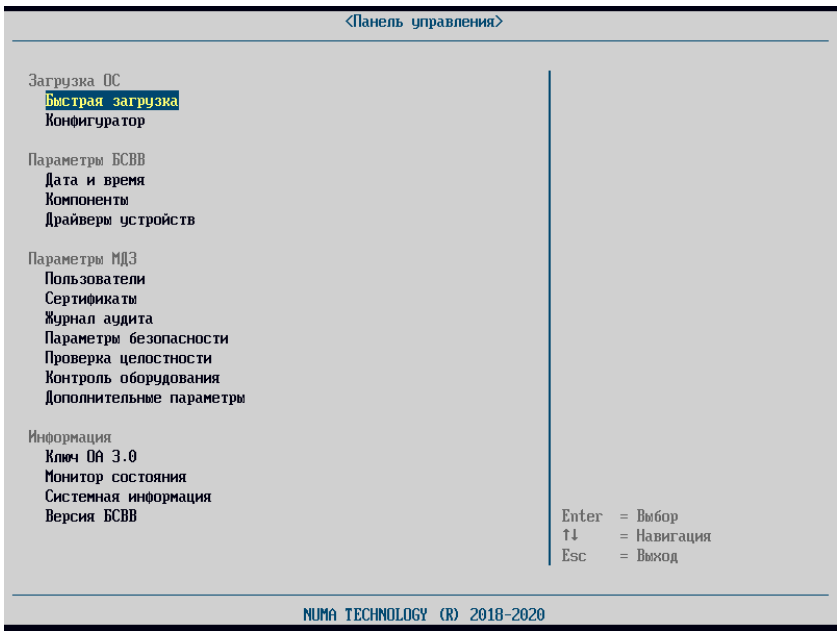

Рисунок 15 – Меню «Панель управления». Вид администратора

Администратору с правами аудитора доступны только два пункта меню (см. рисунок 16):

– «Журнал аудита»;

– «Проверка целостности».

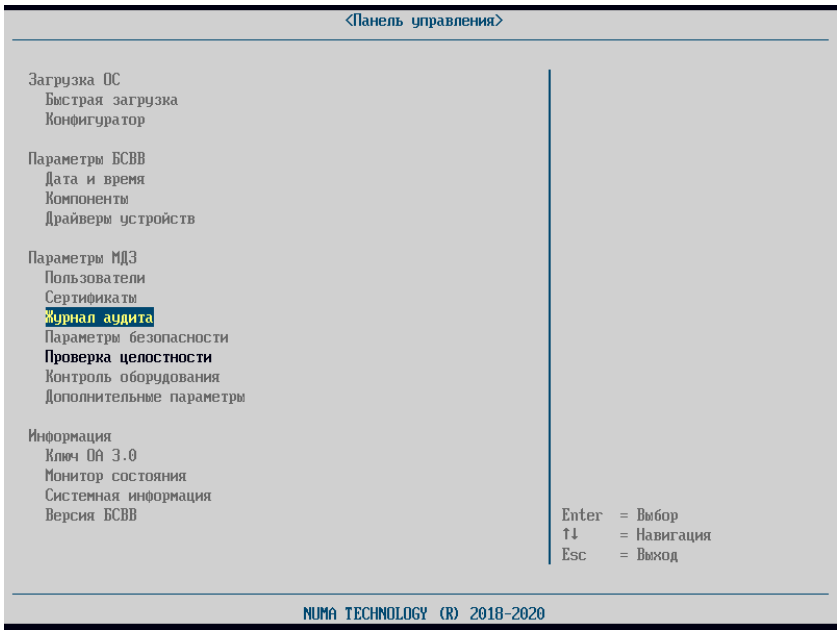

Рисунок 16 – Меню администратора с правами аудитора

5.5. Раздел «Загрузка ОС»

5.5.1. «Быстрая загрузка»

Пункт «Быстрая загрузка» (см. рисунок 17) отображает список доступных носителей и режимов загрузки. Администратору доступен выбор следующих видов загрузки:

– «EFI-авто» – загрузка с различных устройств в соответствии со спецификацией UEFI (http://www.uefi.org/specs/);

Также в этом разделе отображаются носители, определенные через EFI-переменные. Например, для Windows будет отображаться строка «Windows Boot manager».

– «EFI-файл» – администратор может выбрать файл EFI-загрузчика или EFI-приложения для загрузки ОС;

– «Профили загрузки» – показывает существующие профили;

– «Сканировать носители» позволяет обновлять список загрузочных устройств. Необходим для отображения только что подключенных USB-носителей.

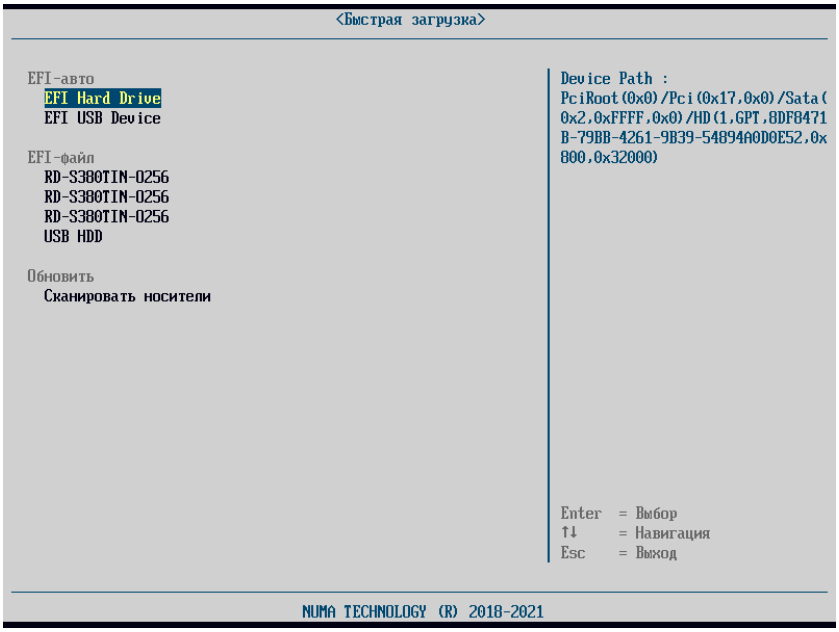

Рисунок 17 – Меню «Быстрая загрузка»

Для загрузки ОС необходимо выбрать вариант загрузки и нажать клавишу «Enter». ОС будет загружена с выбранного устройства.

5.5.2. «Конфигуратор»

Настройка конфигурации загрузки (набора параметров, задающих режим, и источник загрузки) осуществляется из пункта «Конфигуратор» меню «Панель управления» (см. рисунок 18).

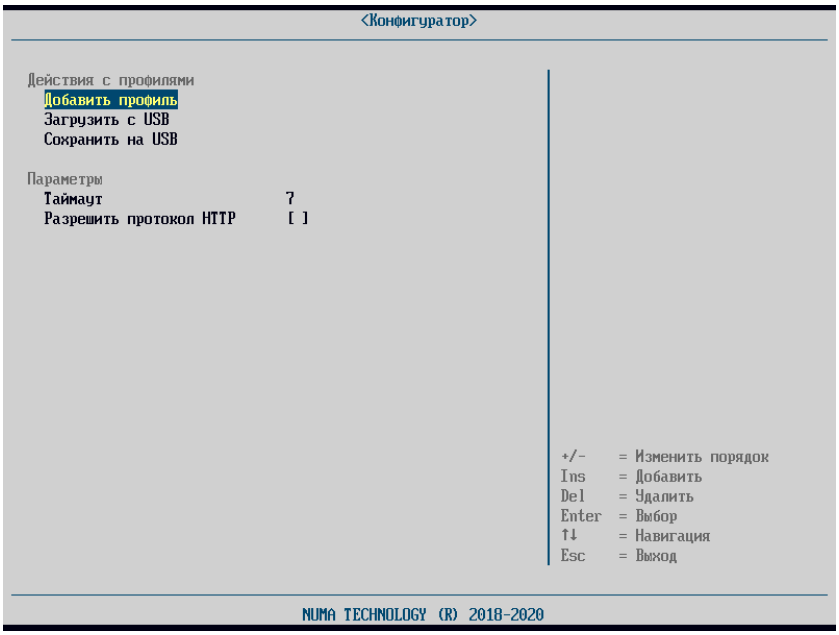

Рисунок 18 – Меню «Конфигуратор»

Операции управления конфигурациями загрузки осуществляются из основного пункта меню «Конфигуратор», которое содержит три раздела: «Профили загрузки»,

«Действия с профилями», «Параметры» (см. рисунок 18).

«Профили загрузки» содержит информацию о созданных ранее профилях загрузки. Если созданных профилей в Изделии нет, то пункт меню не отображается.

«Действия с профилями» содержит следующие подпункты:

– «Добавить профиль» – создание нового профиля загрузки;

– «Загрузить с USB» – импорт уже существующих профилей загрузки;

– «Сохранить на USB» – экспорт созданных профилей загрузки на USB-накопитель.

Параметр «Таймаут» предназначен для управления временем отображения главного меню до начала старта загрузки ОС из первого профиля. Может принимать значения от 1 до 30 секунд. При попытке ввода значения, не попадающего в данный интервал, автоматически восстановится текущее значение таймаута. Величина этого параметра отображается в счетчике обратного отсчета на форме «Главного меню». Работа счетчика останавливается при нажатии на любую клавишу. После этого выбор и загрузка может осуществиться только вручную.

Параметр «Разрешить протокол HTTP» позволяет осуществлять загрузку по сети при помощи незащищенного протокола http. Данный параметр необходимо использовать только для тестирования HTTP Boot. По умолчанию загрузка ОС при профиле загрузки с HTTP Boot осуществляется по защищенному протоколу https.

5.5.2.1. Создание нового профиля загрузки

Для создания новой конфигурации профиля загрузки необходимо нажать кнопку «Ins» или выбрать пункт «Добавить профиль» и заполнить необходимые поля:

– «Имя профиля» – имя профиля, отображаемое в «Главном меню»;

– «Тип загрузки» – необходимо выбрать возможное загрузочное устройство. Доступны следующие типы загрузки:

– EFI-загрузка (присутствует файл efi\boot\bootx64.efi). Отображается строкой «USB Hard Drive» или «EFI USB Device»;

– Пользовательский тип - позволяет выбрать альтернативный EFI-загрузчик или настроить Linux-загрузку (если данный параметр включен в «Компонентах»);

– HTTP Boot – загрузка полезной нагрузки по сети по протоколу HTTPS. Подробный процесс настройки профиля загрузки с типом загрузки HTTP Boot описан в п. 5.5.2.2.

***Примечание**. В зависимости от подключенных типов устройств наличие того или иного типа загрузки может отсутствовать.*

– «Контроль целостности» – добавление нового файла в список проверяемых перед загрузкой ОС;

Пункт «Контроль целостности» доступен для настройки только после первого сохранения созданного профиля загрузки и отображается серым цветом.

– «Сохранить профиль» – сохранение настроек профиля загрузки.

***Примечание**. Пример создания и настройки профиля загрузки с ОС Windows (или другой ОС) через USB-носитель приведен в Приложении 6.*

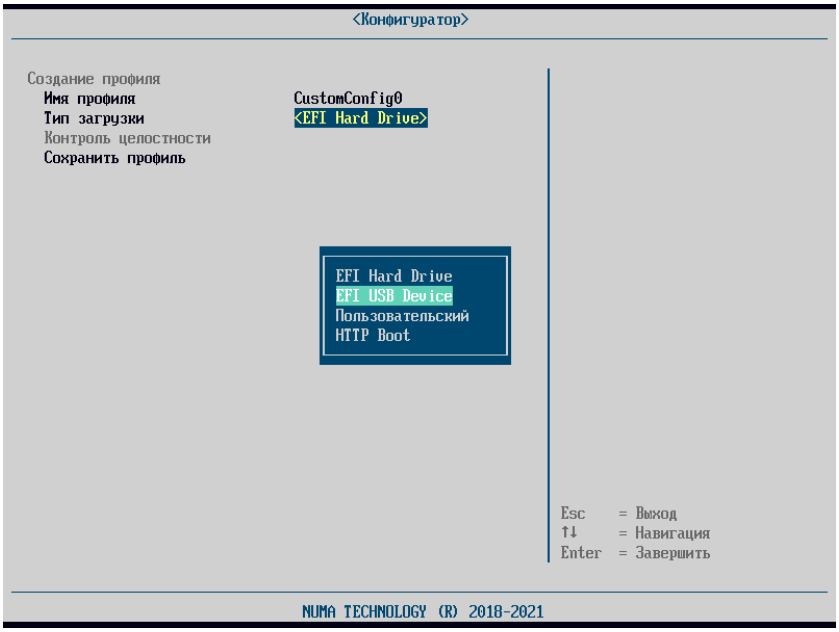

Рисунок 19 – Выбор типа загрузки

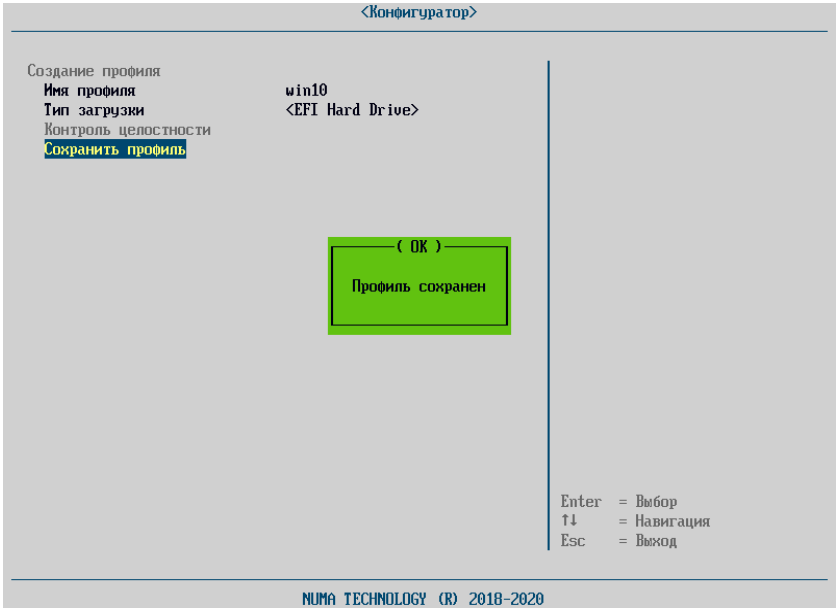

Рисунок 20 – Созданный профиль загрузки

Управление существующими профилями загрузки осуществляется в разделе «Профили загрузки» меню «Конфигуратор».

Настройка порядка профилей загрузки в меню «Конфигуратор» осуществляется кнопками + (плюс) и – (минус). Порядок профилей загрузки, настраиваемым в данном меню будет отображаться в том же порядке в меню «Главное меню».

5.5.2.2. Настройка профиля загрузки с типом загрузки HTTP Boot

Для возможности загрузки по HTTP Boot необходимо выполнить следующие действия:

1) для работы с HTTP Boot необходимо включить драйвера сетевого стека UEFI в разделе меню «Компоненты» → «Сетевой стек»;
2) в меню «Конфигуратор» создать профиль загрузки:
3) ввести имя профиля загрузки (произвольное);
4) в качестве типа загрузки выбрать «HTTP Boot»;

5) выбрать сетевой контролер, с помощью которого будет выполняться загрузка. Символом «*» отмечены устройства, к которым подключён сетевой кабель (см. рисунок 21);

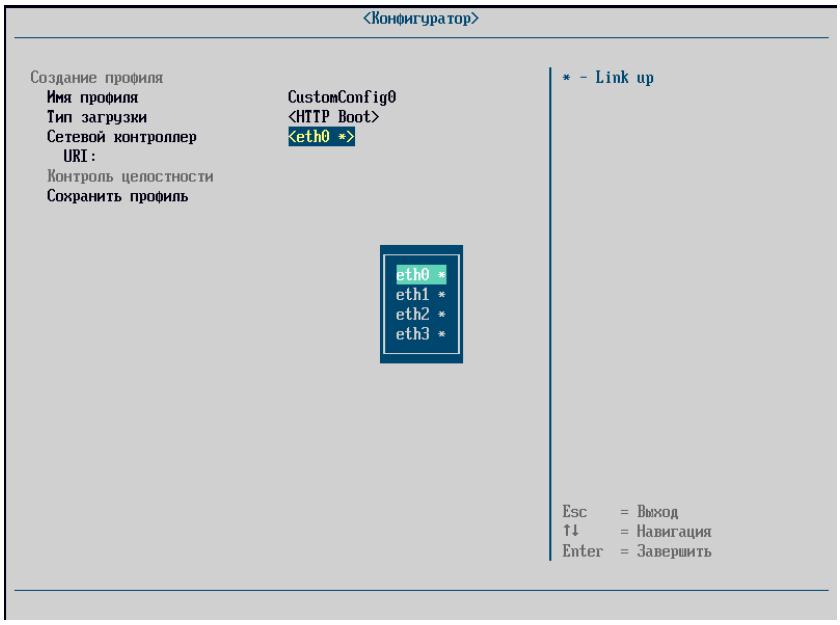

Рисунок 21 – Настройка HTTP Boot. Выбор сетевых контроллеров

6) в поле «URI» указать полный адрес загружаемого образа ОС (см. рисунок 22);

***Примечание**. В случае если порт отличается от стандартных (http – 80, https – 443), необходимо указать порт через двоеточие.*

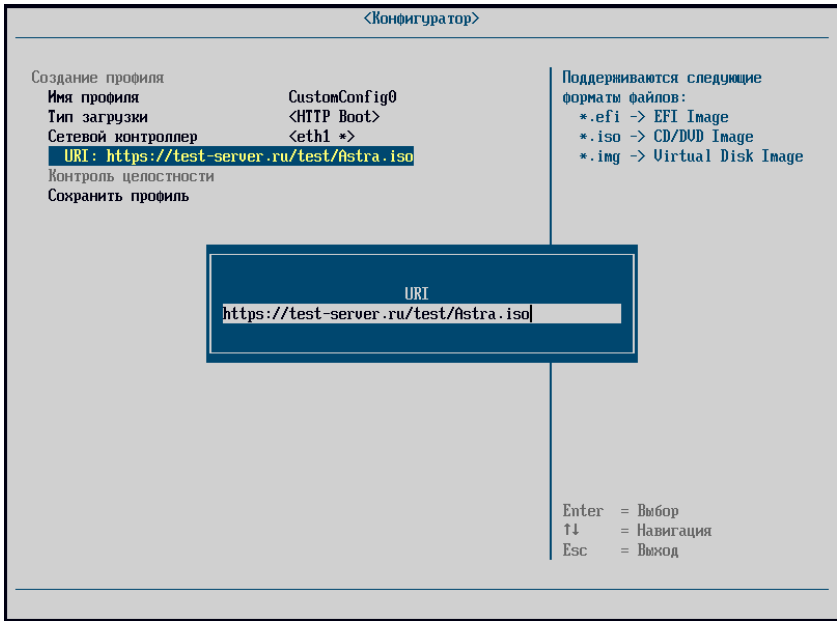

Рисунок 22 – Настройка HTTP Boot. Ввод адреса загрузки

7) загружаемый образ должен иметь электронную цифровую подпись (далее – ЭЦП) для проверки его целостности и подлинности. Файл ЭЦП должен храниться на сервере в том же каталоге, что и загружаемый образ, и иметь наименование и расширение <Filename.iso>.sign, где Filename.iso – имя загружаемого файла ОС.

8) сертификат администратора безопасности для проверки ЭЦП может быть добавлен в локальное хранилище Изделия (см. раздел 5.7.2) или же располагаться на сервере

в том же каталоге, что и загружаемый образ и иметь наименование и расширение <Filename.iso>.crt, где Filename.iso – имя загружаемого файла ОС. Поддерживаются PEM и DER форматы сертификатов.

Корневой сертификат удостоверяющего центра должен быть заранее загружен в локальное хранилище сертификатов, после чего появится возможность загрузки локальных сертификатов администратора безопасности (см. раздел 5.7.2).

Файл сертификата на сервере, аналогично файлу ЭЦП, должен находиться в том же каталоге, что и загружаемый образ, и иметь расширение *.crt.

***Примечание**. Поддерживаются форматы *.efi, *.iso, *.img для загружаемого образа ОС. Файл иного типа загружаться не будут!*

Подпись образа загружаемого файла ОС генерируется администратором на предприятии самостоятельно в доверенной ОС Astra Linux.

Генерация сертификатов, подписей и ключей, включая TLS – являются средствами обеспечения целостности загружаемого образа операционной системы.

9) по умолчанию разрешено только защищенное https соединение. В отладочных целях доступно незащищённое соединение http. Для этого необходимо включить параметр «Разрешить протокол HTTP» в меню «Конфигуратор»;

Внимание! Использование http соединения не в отладочных целях ЗАПРЕЩЕНО.

10) сохранить профиль загрузки;

11) перезагрузить Изделие, запустить созданный профиль.

Во время загрузки созданного профиля сначала выполняется последовательное скачивание файлов образа, подписи и сертификата (файл сертификата загружается при необходимости).

Проверка ЭЦП осуществляется в два этапа:

– с использованием локальных сертификатов, загруженных в «Сертификаты для HTTP Boot». Проверка будет выполняться, пока ЭЦП не будет успешно проверена;

– если ни один локальный сертификат не подошел, будет загружен и использован сертификат с удаленного сервера (CRT-файл).

После успешного выполнения всех процедур будет выполнена загрузка ОС.

При возникновении ошибок необходимо проверить, что сетевой кабель подключён в разъем СВТ, указанный при создании профиля загрузки, включен параметр «Сетевой стек» в меню «Компоненты», убедиться в наличии и правильности всех элементов для загрузки: подписанный файл-образ ОС, файл ЭЦП, файл сертификата для проверки ЭЦП.

5.5.2.3. Удаление профилей загрузки

Для удаления профиля загрузки необходимо перейти на профиль загрузки и нажать кнопку «Del» (см. рисунок 23).

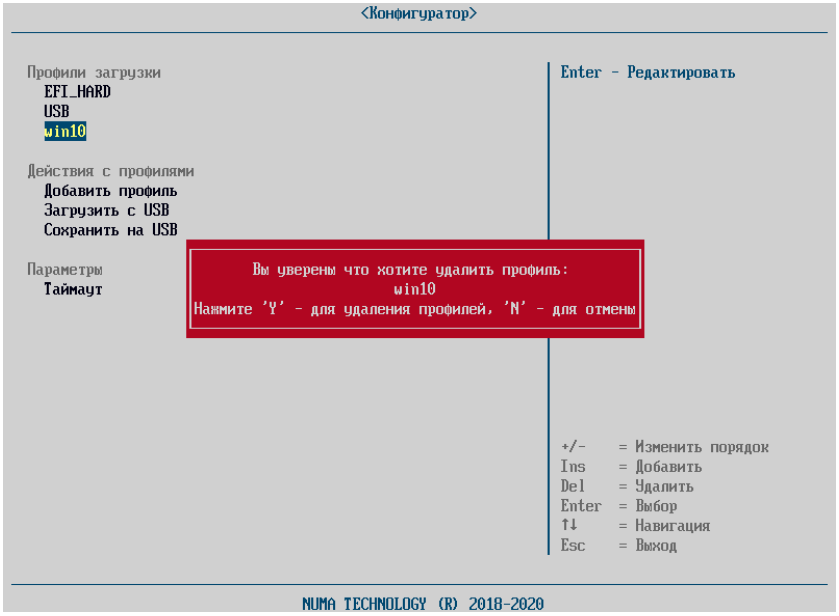

Рисунок 23 – Удаление профиля загрузки

5.5.2.4. Импорт профилей загрузки

Для импорта ранее сохраненных настроек профилей из внешнего файла необходимо перейти в пункт «Загрузить с USB» выполнить следующие действия:

– подключить USB–накопитель с файлом конфигурации;

– выбрать пункт меню «Конфигуратор» → «Загрузить с USB»;

– выбрать требуемый файл из каталога файлов устройства и нажать «Enter».

В случае успешной загрузки конфигурации будет выдано соответствующее сообщение:

```
Конфигурация успешно сохранена!
```

В случае выбора неподходящего файла будет выдано сообщение:

```
Ошибка! Неизвестный формат файла!
```

5.5.2.5. Экспорт профилей загрузки

Для того чтобы экспортировать конфигурацию во внешний файл на USB-накопитель, необходимо перейти в пункт меню «Конфигуратор» и выполнить следующие действия:

– подключить USB-накопитель (с файловой системой формата FAT32);

– выбрать пункт меню «Конфигуратор» → «Сохранить на USB».

В случае успешной выгрузки файла конфигурации будет выдано соответствующее сообщение

```
Сохранение профилей завершено успешно!
```

Файл с конфигурацией будет сохранен в корневом каталоге устройства с именем, соответствующим шаблону

```
BootProfiles[YY-MM-DD].json, где YYMMDD – текущая дата
```

5.5.2.6. Настройка контроля целостности

Настройка контроля целостности профиля загрузки производится в отдельном меню

«Конфигуратор» → <Профиль загрузки> → «Контроль целостности» (см. рисунок 24).

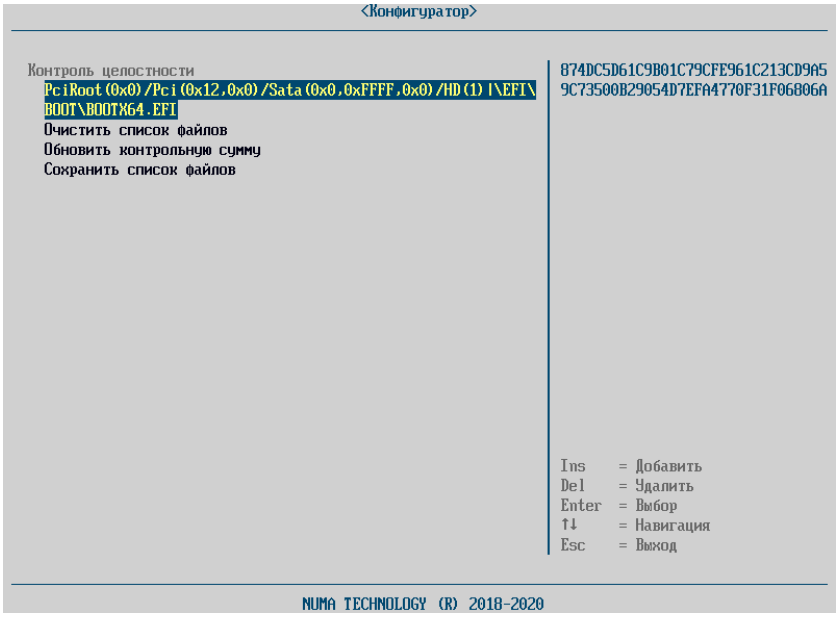

Рисунок 24 – Настройка контроля целостности

Для добавления нового файла в список проверяемых перед загрузкой ОС файлов необходимо выполнить следующие действия:

– нажать клавишу «Ins»;

– выбрать устройство, с которого необходимо добавить файл;

– выбрать требуемый файл и нажать «Enter» – файл появится в списке добавляемых файлов, справа будет выведена его контрольная сумма (см. рисунок 24);

– для удаления файла из этого списка необходимо выделить его и нажать «Enter» (подтверждение не запрашивается); чтобы удалить все файлы из предварительного списка, необходимо выбрать пункт меню «Очистить список файлов»;

– для добавления в список ещё одного файла необходимо вернуться к первому пункту;

– после окончания процедуры добавления файлов следует выбрать пункт меню «Сохранить список файлов» и нажать «Enter». На экране появится сообщение:

```
Список файлов сохранён!
```

Для пересчета контрольной суммы необходимо выбрать пункт «Обновить контрольную сумму» и нажать клавишу «Enter», после чего будет произведено автоматическое обновление контрольной суммы.

***Примечание**. В случае нарушения целостности загружаемого профиля загрузки необходимо выполнить действия, описанные в Приложении 7.*

5.6. Раздел «Параметры БСВВ»

5.6.1. «Дата и время»

Для того чтобы установить системные дату и время необходимо выполнить следующие действия (см. рисунок 25):

– выбрать меню «Дата и время»;

– с помощью клавиш «+» и «–» отредактировать значения;

– выйти из меню с помощью клавиши «Esc».

После выхода из меню данные сохранятся автоматически.

Также доступна автоматическая синхронизация времени при каждом запуске Изделия. Для автоматической синхронизации необходимо включить параметр «Автоматическая синхронизация», а также указать IP-адрес NTP сервера для подключения.

***Примечание**. В Изделии указаны NTP сервера по умолчанию, которые можно изменить.*

Для возможности использования списка доступных NTP серверов из DHCP необходимо включить параметр «Использовать DHCP».

Для принудительной синхронизации необходимо выбрать параметр «Синхронизировать время» и нажать клавишу «Enter».

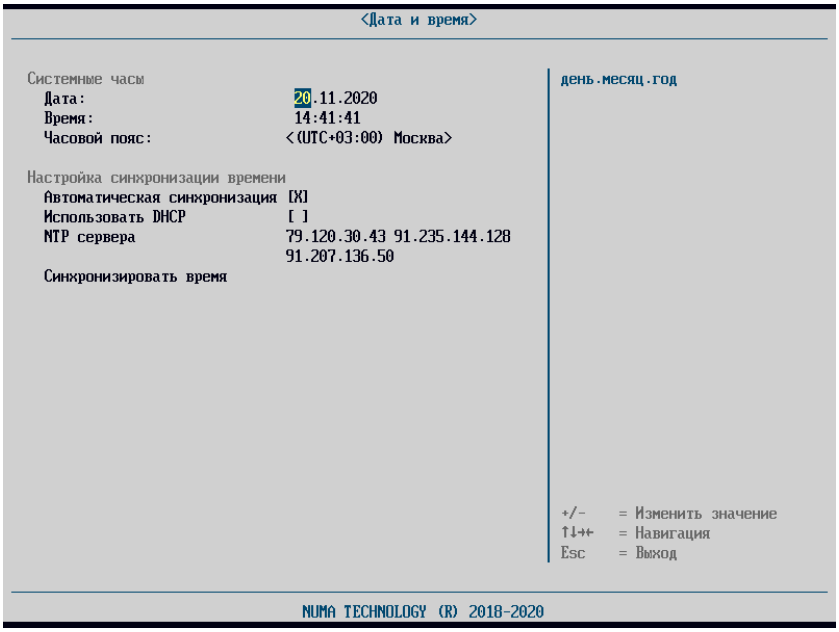

Рисунок 25 – Установка даты и времени

5.6.2. «Компоненты»

***Примечание**. Параметры, отображаемые в данном меню, зависят от типа СВТ, на которое устанавливается Изделие. В разделе перечислены все возможные параметры.*

Меню «Компоненты» предоставляет возможность изменения значений следующих параметров (см. рисунок 26):

– «Удаленный терминал» - разрешение вывода информации в терминал через COM-порт;

– «Видеоадаптер» – определяет порядок выбора видеоадаптера для работы (интегрированный/внешний);

– «GOP – максимальный режим» – подключает максимально возможное разрешение видеоадаптера при запуске ОС;

– «Linux-загрузка» – параметр для активации возможности загрузки драйверов Ext2/Ext4 и добавление тип модуля «Linux» для пользовательской загрузки;

– «Сетевой стек» – параметр для включения/отключения драйверов сетевого стека UEFI для загрузки по сети. Для поддержки протокола версии IPv6 необходимо включить данный параметр;

– «OEM-логотип» – параметр, позволяющий настраивать отображение логотипов при загрузке ОС Windows и ОС Ubuntu в режиме EFI. При включенном параметре в момент загрузки ОС отображается логотип, установленный разработчиком (в зависимости от типа СВТ, на которое установлено Изделие), в случае выключенного параметра отображается стандартный логотип загрузки ОС Windows/ОС Ubuntu;

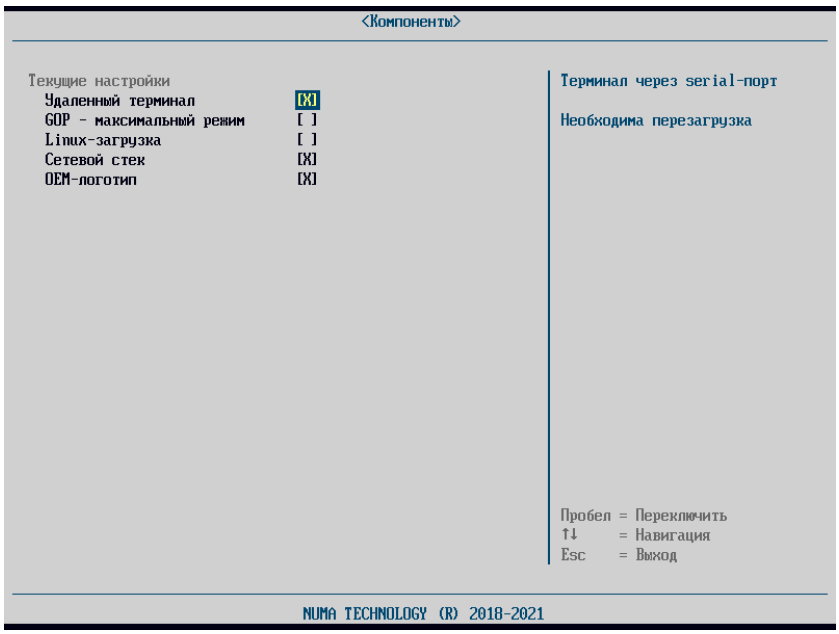

Рисунок 26 – Пункт меню «Компоненты»

5.6.3. «Драйверы устройств»

Данный пункт позволяет просматривать драйверы устройств, установленные на СВТ, проверять правильность их работы и изменять параметры.

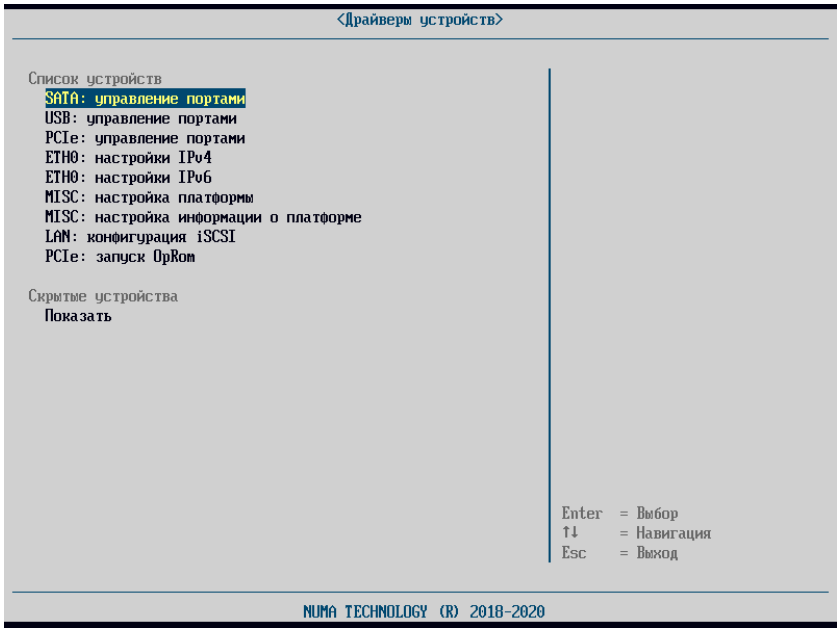

Рисунок 27 – Меню «Драйверы устройств»

Список устройств, отображаемых в диспетчере, зависит от используемого СВТ.

Ниже перечислен список всех возможных настраиваемых параметров.

Для того чтобы настроить параметры платформы, необходимо выполнить следующие действия:

– выбрать пункт меню;
– выбрать пункт, соответствующий требуемому устройству;
– задать необходимые параметры;
– сохранить изменения.

5.6.3.1. CPU: конфигурация

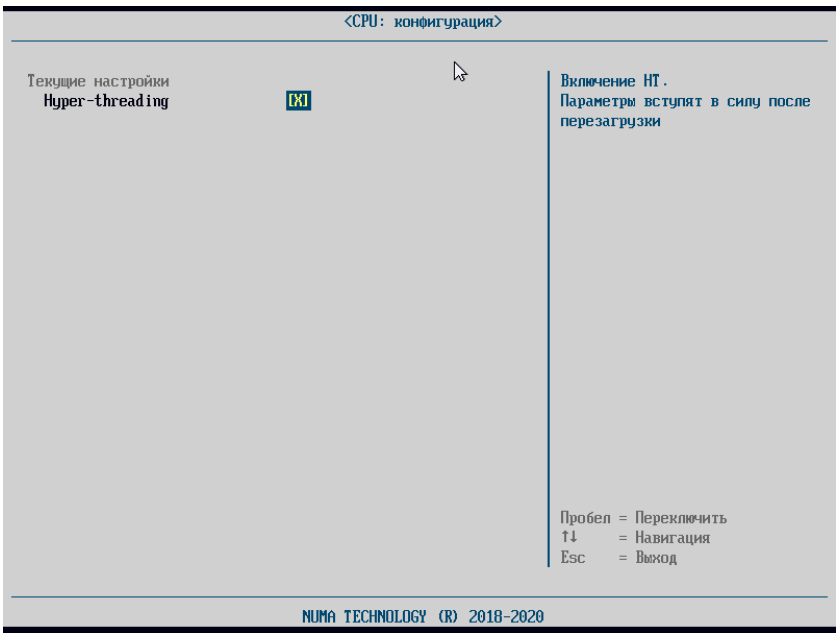

Рисунок 28 – Меню «CPU: конфигурация»

Данный пункт позволяет включать функцию Hyper-threading, которое обеспечивает более эффективное использование ресурсов процессора, позволяя выполнять несколько потоков на каждом ядре.

5.6.3.2. SATA: управление портами

Меню «SATA: управление портами» отображает все доступные SATA-порты и дает возможность администратору отключать/подключать порты.

При отключении SATA-порта, соответственно отключается и устройство, подключенное к этому порту. Эффект отключения можно наблюдать в меню «Быстрая загрузка». Для этого на форме «SATA: управление портами» необходимо отключить SATA-порт, отображаемый в переменной Device Path для подключенного SATA-устройства и **обязательно выполнить перезагрузку**. Подключенное устройство перестанет отображаться на форме «Быстрая загрузка», хотя физически подключено к порту (или к плате кабелями питания и передачи данных).

Кроме этого факт отключения устройства можно увидеть на форме «Системная информация»: если устройство было единственным SATA-устройством, на форме перестанет отображаться раздел «SATA-накопители».

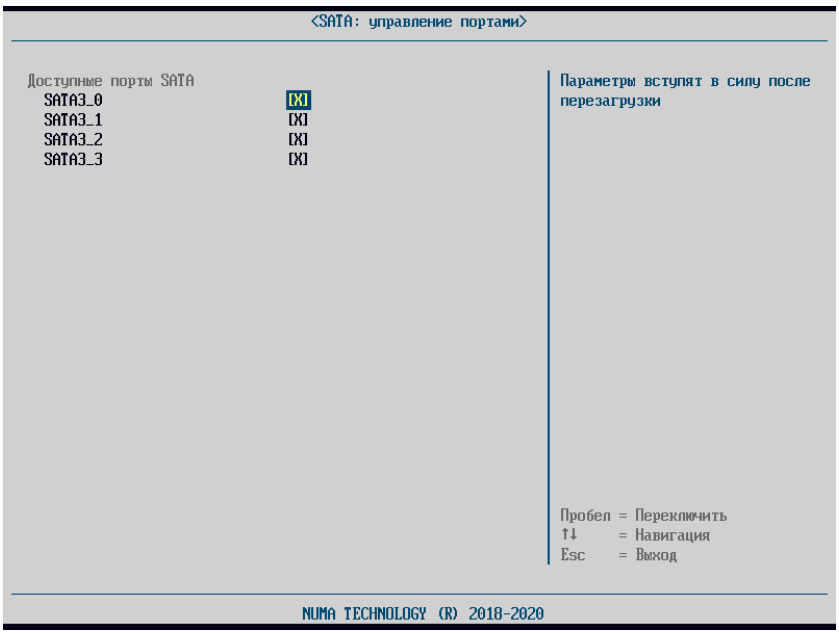

Рисунок 29 – Меню «SATA: управление портами»

5.6.3.3. USB: управление портами

Меню «USB: управление портами» (см. рисунок 30):

– отображает все доступные USB–порты и дает возможность администратору отключать/подключать порты;

– позволяет администратору управлять процессом загрузки с подключенных USB-устройств и при необходимости блокировать загрузку.

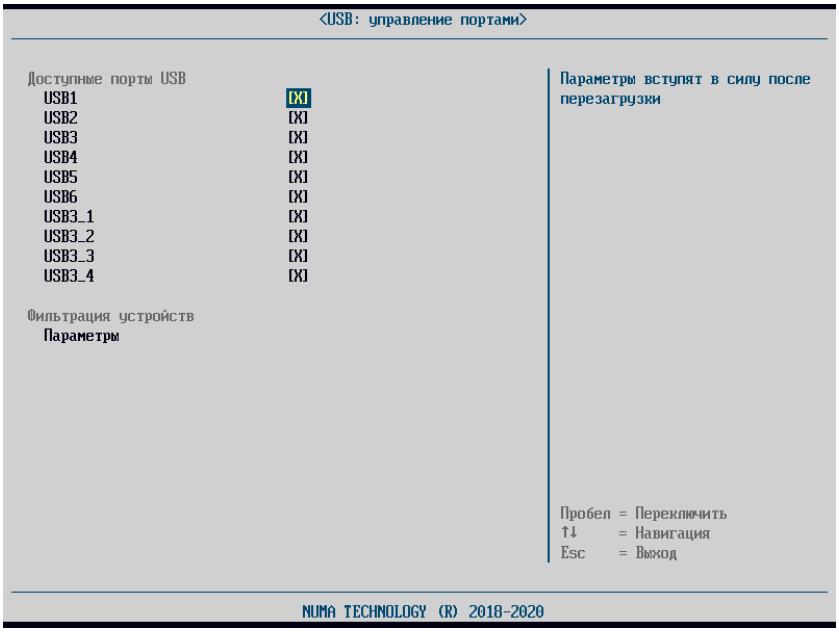

Рисунок 30 – Меню «USB: управление портами»

При отключении USB-порта соответственно отключается и устройство, подключенное к этому порту. Эффект отключения можно наблюдать в меню «Быстрая загрузка». Для этого в меню «USB: управление портами» необходимо отключить USB-порт, отображаемый в переменной Device Path для подключенного USB-устройства и **обязательно выполнить перезагрузку**. Подключенное устройство перестанет отображаться в меню «Быстрая загрузка», хотя физически остается подключенным к порту.

Кроме раздела управления доступностью USB-портов, в меню есть раздел

«Фильтрация устройств». Фильтр может блокировать работу USB-устройств определенных категорий (см. рисунок 31).

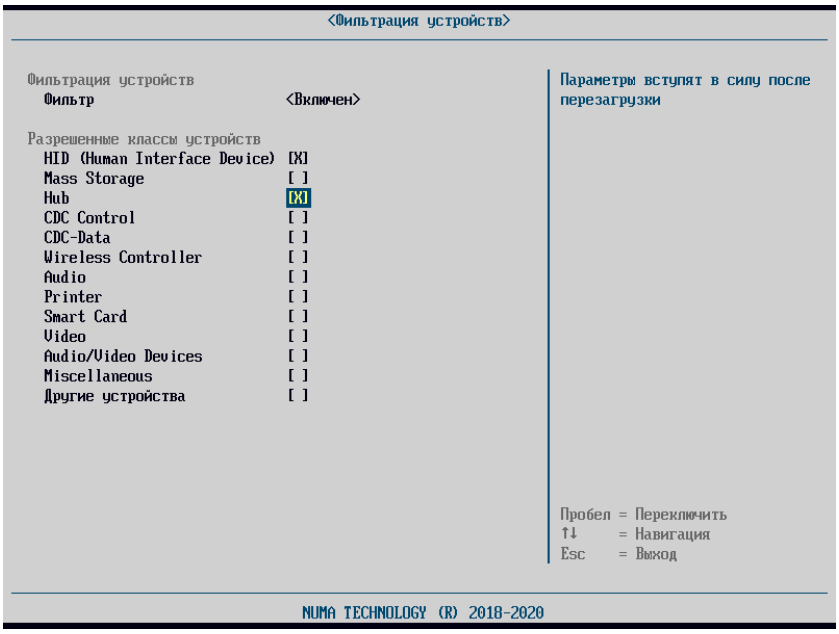

Рисунок 31 – Настройка фильтра

К USB HID (human interface device) устройствам относятся USB-клавиатура и USB-мышь, USB-джостик.

К Mass Storage относятся USB-накопители;

К Hub относятся USB-хабы;

К CDC Control относятся модем, сетевая карта, COM-порт;

CDC-Data используется совместно с классом CDC;

К Wireless Controller относится Bluetooth-адаптер;

К Audio относится звуковая карта, MIDI;

К Printer относятся принтеры и сканеры;

К Smart Card относится карты памяти;

К Video относятся веб-камеры;

Audio/Video Devices относятся аудио-видео устройства;

К Miscellaneous относятся ActiveSync-устройства;

Другие устройства.

В случае отключения класса устройств «Mass Storage», попытка осуществить загрузку с USB-носителя в меню «Быстрая загрузка» или при старте Изделия (если в меню «Конфигуратор» для подключенного носителя выбрано действие – «Загрузить с USB»), приведет к ошибке и автоматической перезагрузке Изделия. Дополнительно к этому, после перезагрузки USB-порт будет отключен до момента следующей перезагрузки СВТ.

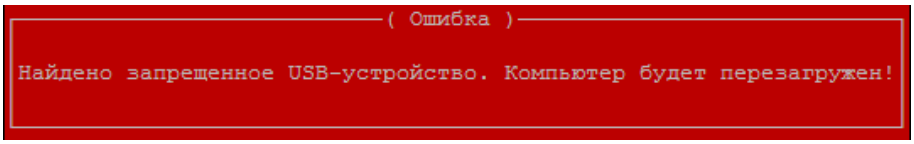

Рисунок 32 – Сообщение об ошибке

Примечание. *При отключении класса устройств «Hub» и в случае подключения*

USB-устройства вместе с HID-устройствами к одному USB-хабу, будет заблокирована работа всех устройств, подключенных к USB-хабу.

5.6.3.4. PCI: управление портами

Меню «PCI: управление портами» отображает все доступные PCI-порты и дает возможность администратору отключать/подключать порты, с помощью механизма чекбоксов. При отключении PCI-порта соответственно отключается и устройство, подключенное к этому порту. Эффект отключения можно наблюдать в меню «Быстрая загрузка». Для этого в меню «PCI: управление портами» отключить PCI-порт, отображаемый в переменной Device Path для подключенного PCI-устройства и **обязательно выполнить перезагрузку**. Подключенное устройство перестанет отображаться в меню «Быстрая загрузка», хотя физически подключено к порту (плате кабелями питания и передачи данных). Кроме этого факт отключения устройства можно увидеть на форме «Системная информация»: если устройство было единственным PCI-устройством, на форме перестанет отображаться раздел [PCI-накопители].

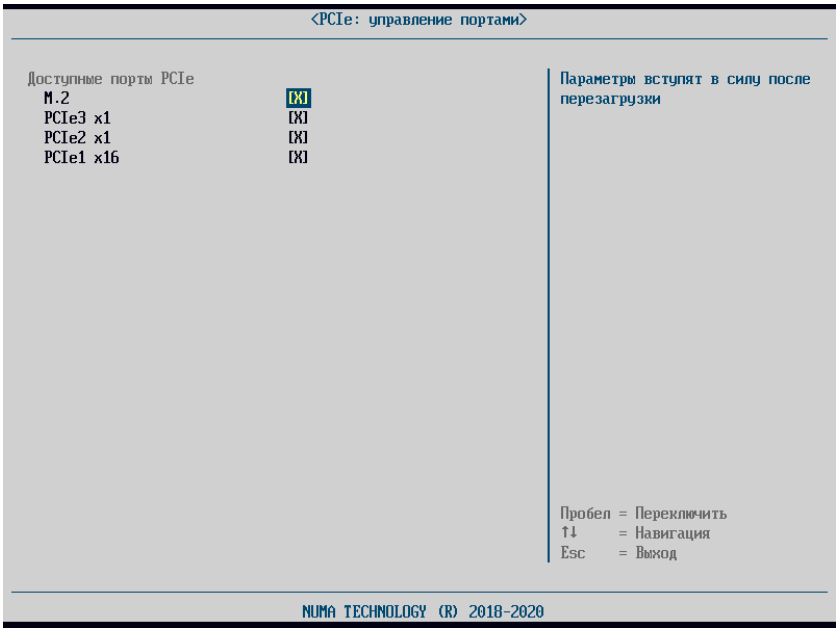

Рисунок 33 – PCI: управление портами

5.6.3.5. ETH0: настройка IPv4

Данный пункт предназначен для настройки работы сетевых протоколов (TCP/UDP) IPv4. Вид меню представлен на рисунке 34.

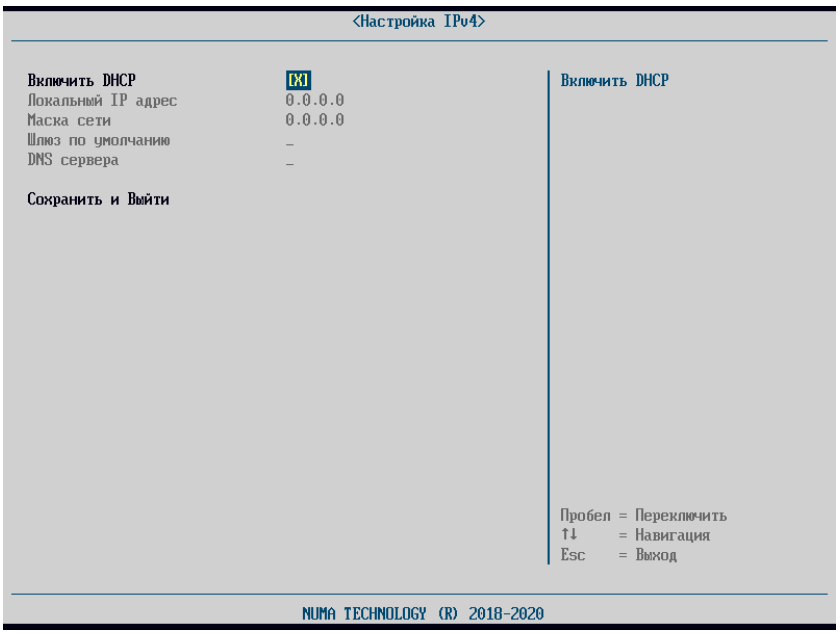

Рисунок 34 – Меню настройки IPv4

Поддерживается два режима настройки:

– автоматический - с использованием DHCP (Dynamic Host Configuration Protocol), протокол динамической настройки хостов;

– режим ручной настройки - настраивается системным администратором.

Заполнение каждого поля сопровождается подсказками с примерами заполнения. Например, для «DNS сервера»: «Введите адреса DNS серверов через пробел. Пример: 192.168.10.8 192.168.10.9».

По умолчанию в Изделии установлен режим работы с использованием DHCP.

5.6.3.6. ETH0: настройка IPv6

Данный пункт предназначен для настройки работы сетевых протоколов (TCP/UDP) IPv6. Вид формы представлен на рисунке 34.

> ***Примечание**. Данная настройка появляется только при включенном параметре «Сетевой стек. IPv6» меню «Компоненты».*

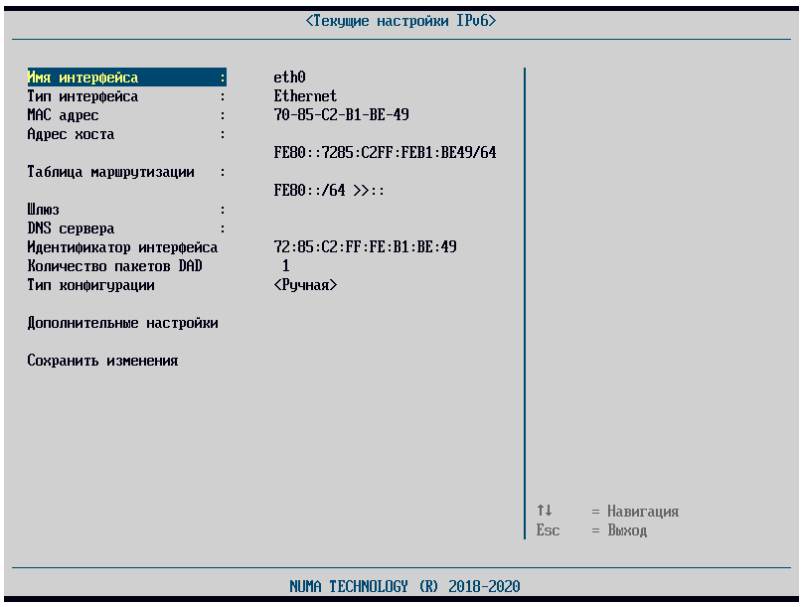

Рисунок 35 – Меню настройки IPv6

Для настройки необходимо заполнить следующие параметры:

– идентификатор интерфейса – альтернативный 64-битный идентификатор;

– количество пакетов DAD – количество последовательных пакетов опроса соседей (NSm), отправленных при поиске дублированного адреса. При параметре 0 обнаружение дублированного адреса не выполняется;

– тип конфигурации – доступные параметры <автоматическая> и <ручная>;

– дополнительные настройки (см. рисунок 36).

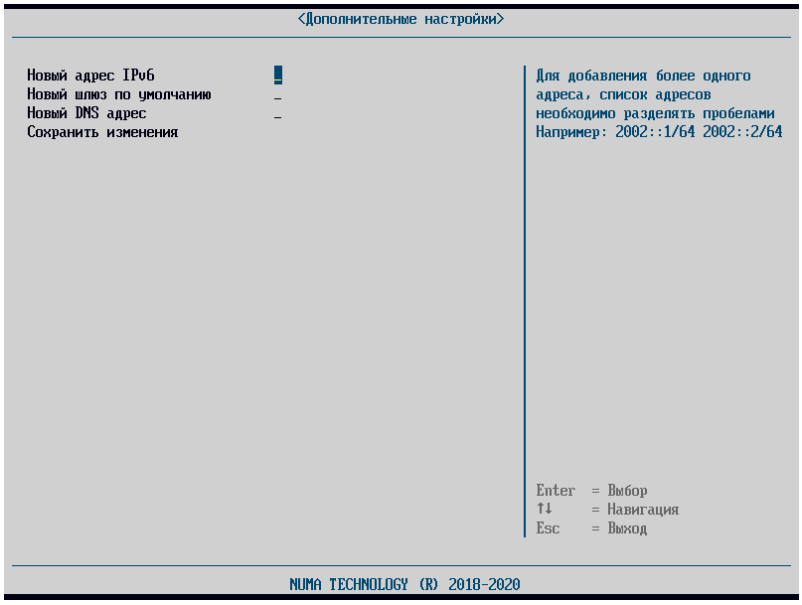

Рисунок 36 – Дополнительные настройки IPv6

5.6.3.7. MISC: настройка платформы

Параметры для настройки данного раздела отличаются в зависимости от типа СВТ, на которое установлено Изделие. В разделе перечислены все доступные параметры настройки.

5.6.3.7.1. Аварийное включение

Данный пункт предназначен для настройки поведения Изделия в случае аварийного

выключения питания (см. рисунок 37).

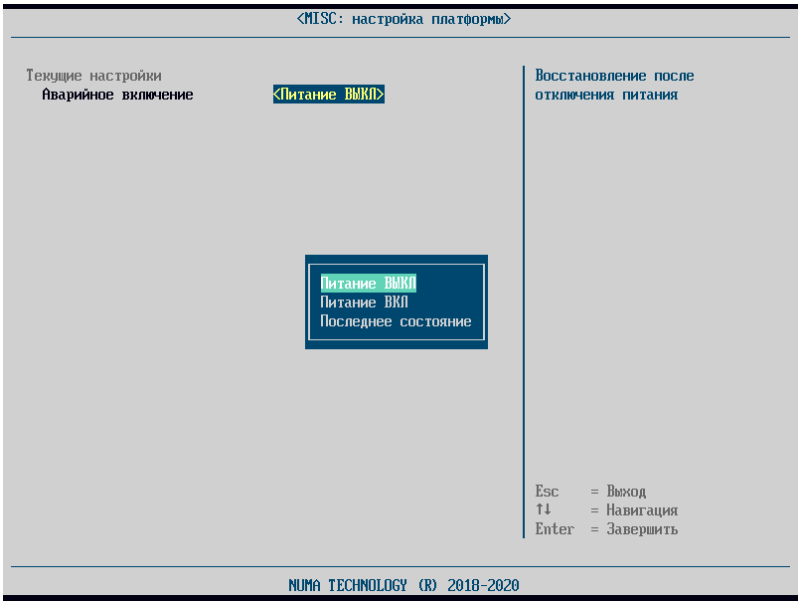

Рисунок 37 – Меню управления параметрами настройки платформы

В зависимости от установленного значения настройки, после аварийного отключения питания плата:

– при значении <Питание ВКЛ> будет автоматически включаться при восстановлении питания;

– при значении <Питание ВЫКЛ> не будет автоматически включаться при восстановлении питания.

5.6.3.7.2. Режим Wake on LAN/PCIE

Настройка параметра «Wake on LAN/PCIE» позволяет отключать/включать СВТ посредством отправки через локальную сеть специального сигнала на сетевой адаптер и PCIe-порты.

***Примечание**. Изменение параметра вступает в силу сразу без перезагрузки системы.*

5.6.3.7.3. Режим Wake on RTC

Параметр «Wake on RTC» отвечает за автоматическое включение питания компьютера в заданное время по сигналу от часов RTC (см. рисунок 38).

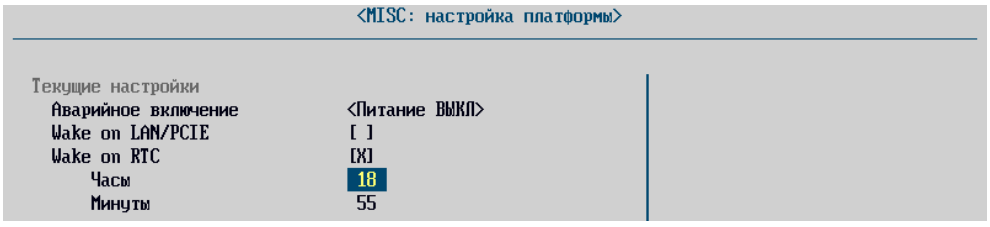

Рисунок 38 – Параметр «Wake on RTC»

***Примечание 1.** Изменение параметра вступает в силу сразу без перезагрузки системы.*

***Примечание 2.** Данная настройка работает только при условии выключения СВТ штатным образом (по кнопке). При отключении шнура от блока питания*

настройка не срабатывает.

5.6.3.7.4. Настройка интерфейса I2C для тачпада

Данный пункт предназначен настройки работы тачпада в ОС Astra Linux Common Edition v1.6. Для стабильной работы тачпада в ОС Astra Linux необходимо отключить параметр «Интерфейс i2c для тачпада».

Данный пункт меню не влияет на работу тачпада в иных ОС.

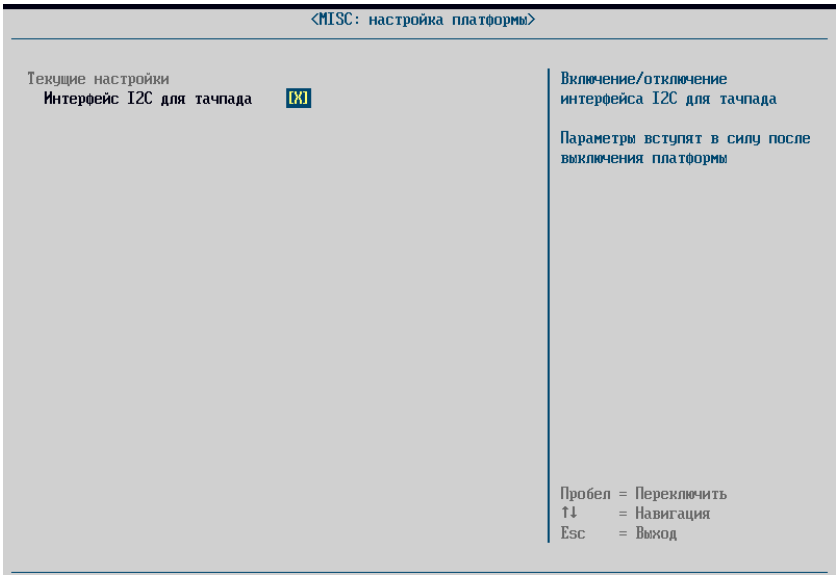

Рисунок 39 – Меню управления параметрами настройки платформы

5.6.3.7.5. Режим SATA-контроллера

Данный пункт предназначен для настройки работы SATA-контроллеров. Доступно два режима работы SATA-контроллера:

– AHCI – стандартный режим работы контроллера;

– RAID – возможность объединять несколько накопителей в RAID-массивы с целью повышения надежности хранения информации или для увеличения скорости работы.

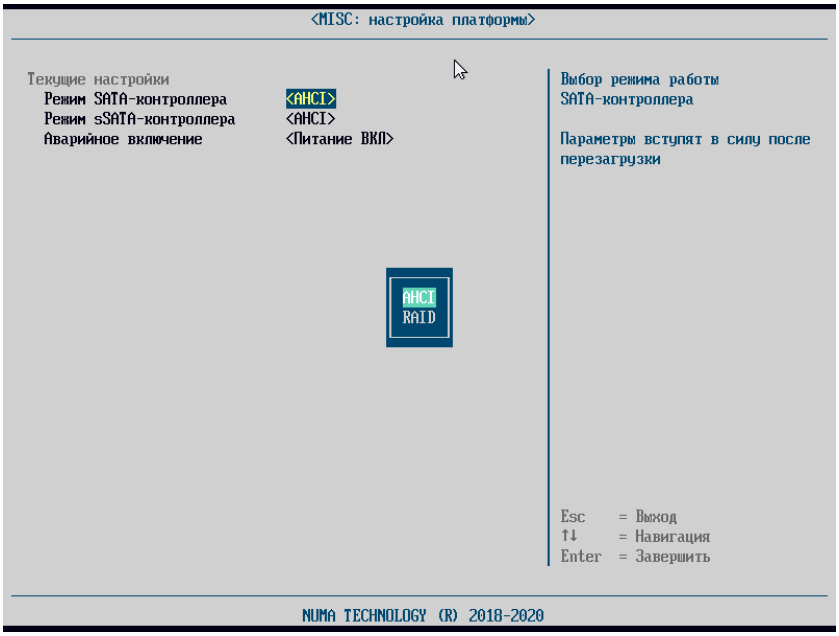

Рисунок 40 – Меню настройка платформы

Примечание. *Управление RAID-массивами осуществляется в ПО «Intel RST».*

Для выбора режима необходимо используя клавиши навигации выбрать режим, нажать клавишу «Enter» для подтверждения выбора.

RAID-массив отображается в списке загрузочных устройств с названием, определенном при создании массива (см. рисунок 41).

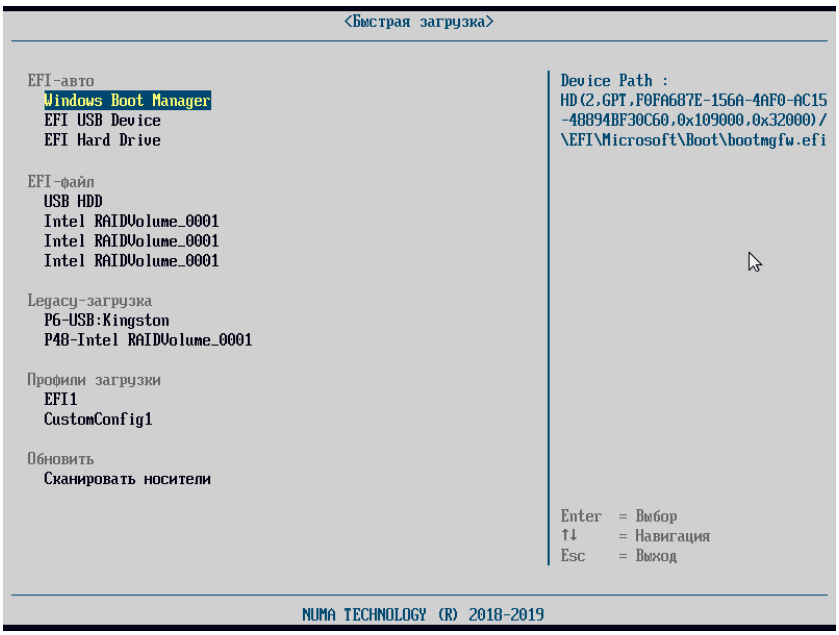

Рисунок 41 – Отображение RAID-массивов

5.6.3.7.6. WiFi- адаптер

При отключении параметра «WI-FI адаптер» в настройках загруженной операционной системы перестанет отображаться сетевой адаптер WI-FI.

5.6.3.7.7. Контроллер HD-Audio

При отключении параметра «Контроллер HD-Audio» в настройках загруженной операционной системы перестанет отображаться контроллер HD-Audio.

5.6.3.7.8. Настройка режима управления вращением вентиляторов

Данное меню позволяет настроить режим работы вентилятора для процессора (CPU FAN) и системного вентилятора (SYS FAN).

Для настройки доступны два режима работы:

– Автоматический – автоматическая регулировка оборотов (см. рисунок 42);

– Ручной – Изделие поддерживает обороты, указанные в данном поле (см. рисунок 43).

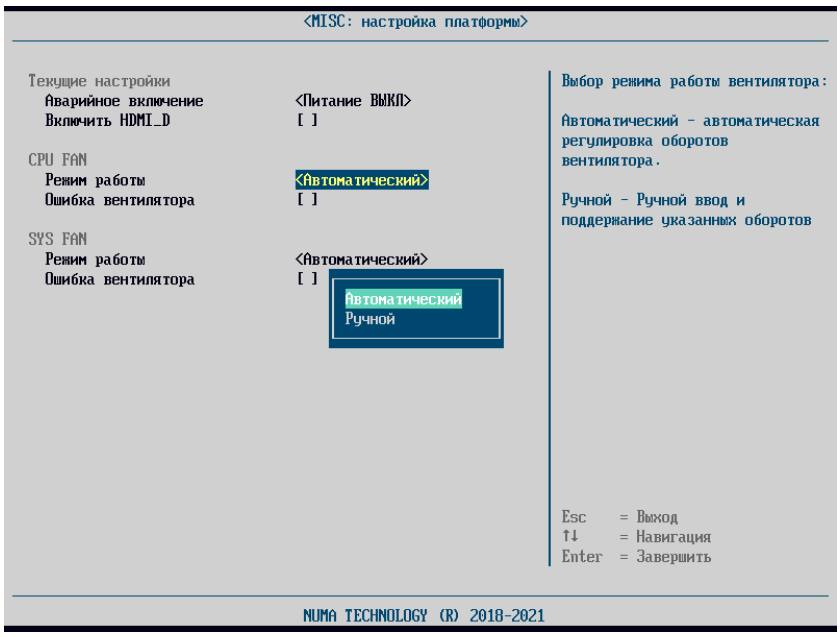

Рисунок 42 – Настройка режима работы вентиляторов. Режим «Автоматический»

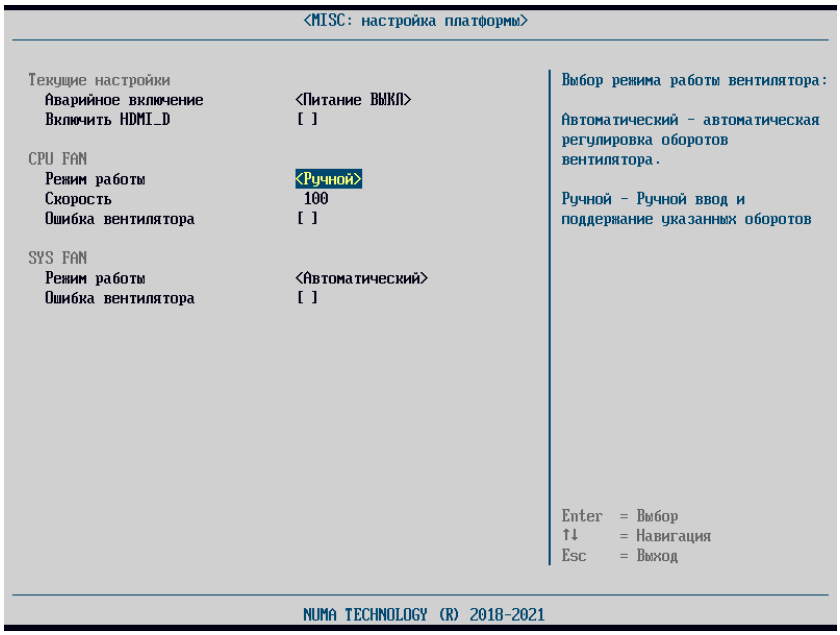

Рисунок 43 – Настройка режима «Ручной»

Параметр «Ошибка вентилятора» позволяет настраивать отображение ошибки в случае отсутствия оборотов вентилятора.

При включении СВТ отображается ошибка:

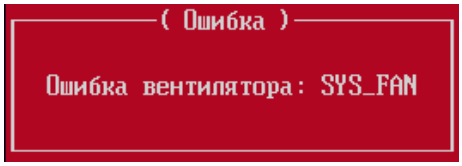

Рисунок 44 – Пример вывода ошибки «Ошибка вентилятора: SYS_FAN»

5.6.3.8. MISC: настройка информации о платформе

Пункт позволяет присвоить СВТ, на которое установлено Изделие, инвентарный номер.

Для присвоения инвентарного номера необходимо ввести данные в поле

«Инвентарный номер» длиной до 15 символов. Данные будут сохранены после перезагрузки СВТ.

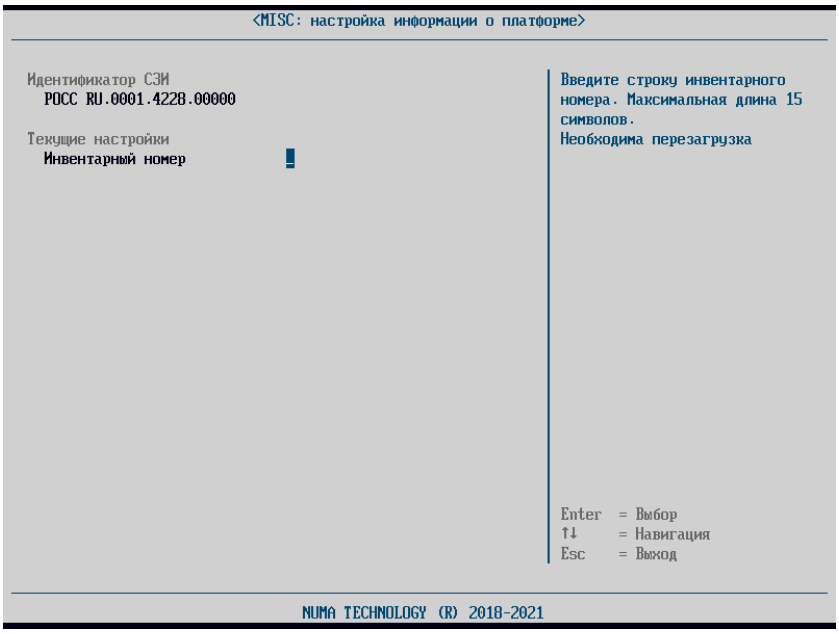

Рисунок 45 – Настройка информации о системе

Информацию об инвентарном номере можно наблюдать в форме «Системная информация» (см. рисунок 107).

Автоматически при активации лицензии на право использования Изделия в данном меню отображается идентификатор СЗИ – идентификатор средства защиты информации, являющаяся уникальным параметром для каждой поставки Изделия.

Идентификатор СЗИ имеет следующий формат РОСС RU.0001.4228.XXXXXX, где:

– первая группа знаков содержит прописные буквы и цифры РОСС RU.0001, указывающие на систему сертификации ФСТЭК России;

– вторая группа знаков указывает на номер сертификата соответствия Изделия в системе сертификации ФСТЭК России;

– третья группа знаков указывает на номер лицензии в системе учета средств защиты информации, произведенных ООО «НумаТех».

5.6.3.9. LAN: конфигурация iSCSI

Поддержка iSCSI протокола позволяет загружать ОС с сетевого диска.

Для настройки драйвера необходимо:

– в меню «Компоненты» включить «Сетевой стек»;

– подключить сетевой кабель к сетевому порту (например, LAN1);

– ввести имя инициатора iSCSI в виде iqn (iSCSI Qualified Name): буквенная аббревиатура iqn; дата (гггг-мм), когда блок присвоения имен завладел доменом; имя домена в обратном порядке (org.example); необязательное ":" служащее префиксом для имени хранилища, указанного блоком присвоения имен (см. рисунок 46).

Например: iqn.2019-12.com.example:storage:disk2.sys.prof

– войти в меню соответствующего сетевого порта (LAN1), включить настройки «Включить iSCSI», «Включить DHCP» (см. рисунок 47);

– при указании «Автоматическая настройка» параметры iSCSI будут получены с DHCP-сервера;

Примечание. *Необходимо настроить на сервере DHCP option 17.*

– для ручной настройки необходимо заполнить всю необходимую информацию iSCSI Target: имя, IP-адрес, порт, LUN (опционально) и CHAP (тип аутентификации);

– сохранить созданные настройки.

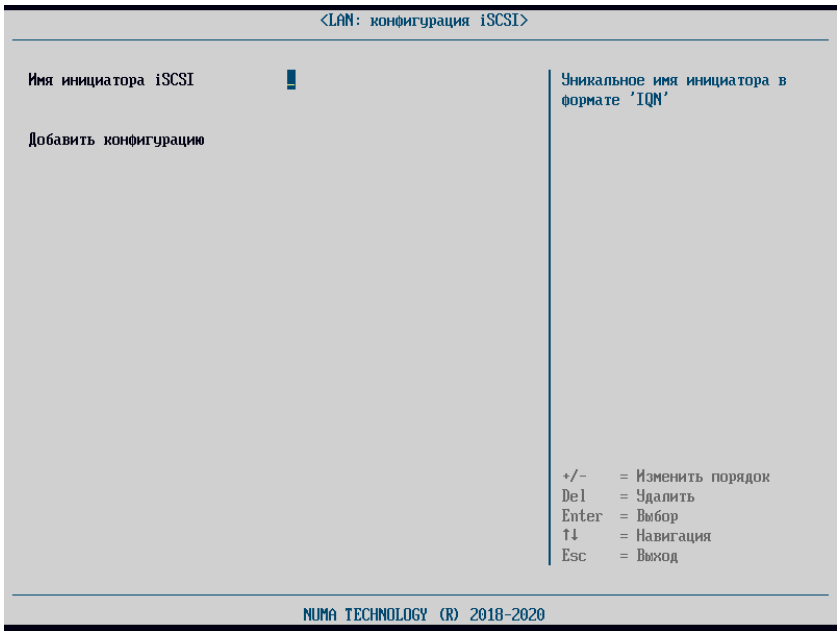

Рисунок 46 – LAN: конфигурация iSCSI

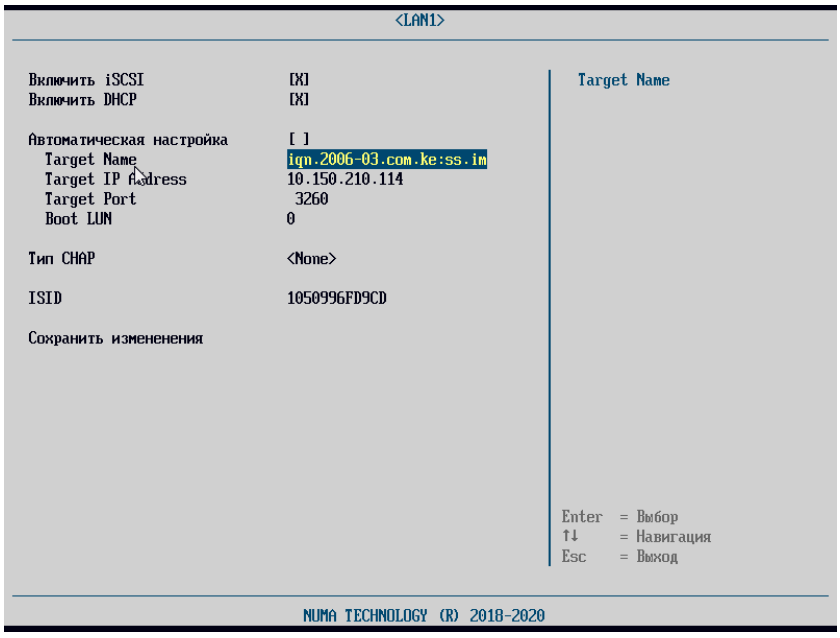

Рисунок 47 – Настройка параметров сетевого порта

После перезагрузки Изделия сетевой диск iSCSI будет доступен для загрузки в режиме EFI/Linux.

Примечание*. Диск должен содержать разделы с поддерживаемой файловой системой.*

5.6.3.10. PCIe: запуск OpRom

Данный пункт необходим для настройки запуска OpRom внешних PCIe устройств. Для включения параметра необходимо перейти в пункт «PCIe: запуск OpRom», в появившейся форме добавить устройство, выбрав действие «Добавить» в разделе «Действия с устройствами». На форме «Добавление устройства» отобразится идентификатор подключенного устройства и тип поддерживаемой загрузки (EFI). Добавленную запись необходимо сохранить. По умолчанию запуск OpRom разрешен.

Примечание 1. *В случае поддержки устройством обоих типов загрузки одновременно, необходимо добавить отдельную запись для каждого типа загрузки.*

Примечание 2. *Значение настройки <Запуск OpRom> для конкретного устройства, имеет больший приоритет, чем значение настройки «Запуск OpRom по умолчанию».*

В разделе «Дополнительно» устанавливается настройка параметра OpRom (см. рисунок 48).

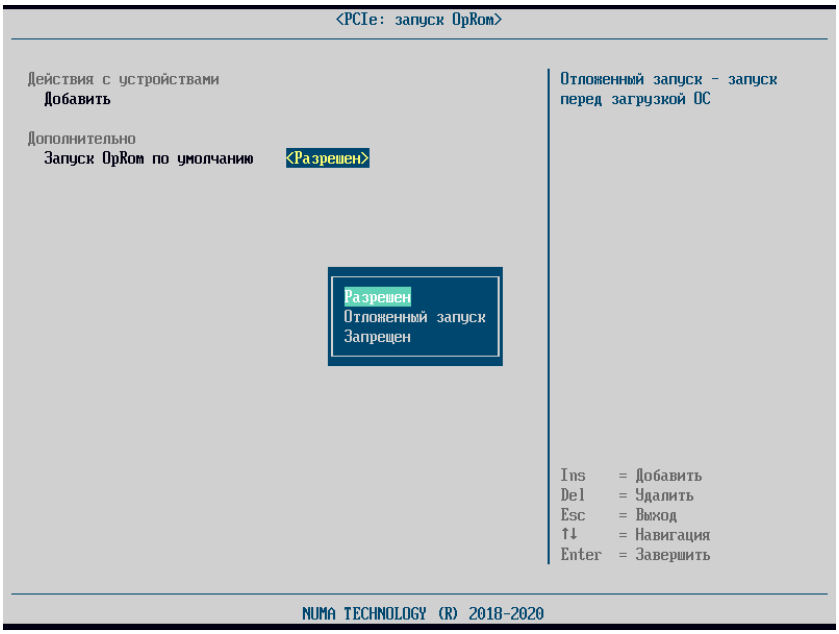

Рисунок 48 – Настраиваемые параметры запуска OpRom

Параметр может принимать три значения:

– «Разрешен» – OpRom устройство должно успешно отработать;

– «Запрещен» – OpRom устройство не должно отработать;

– «Отложенный запуск» – OpRom устройство должно успешно стартовать при передаче управления (загрузке) ОС.

Список совместимых PCIe устройств определен в приложении 3 настоящего документа.

5.6.3.11. SATA: контроль доступа

Форма предназначена для управления доступом к подключенным SATA-устройствам (см. рисунок 49).

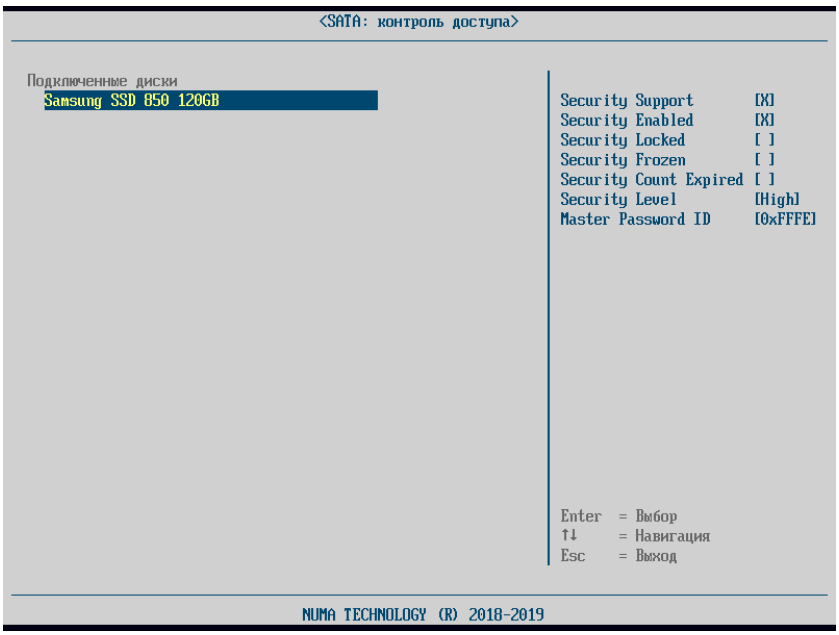

Рисунок 49 – Форма для управления доступа к подключаемым устройствам

На подключенные жесткие диски можно установить пароль для доступа. Если пароль не введен, диск будет недоступен для использования.

Пароли вводятся парой – User/Master: User-пароль позволяет ставить и снимать защиту с жесткого диска, Master-пароль позволяет сбрасывать User-пароль в случае его потери. Поддерживается два уровня защиты:

– High level – сброс User-пароля происходит без стирания информации с жесткого диска;

– Maximum level - сброс User-пароля происходит только после полного стирания жесткого диска.

Для установки защиты, необходимо:

– выбрать необходимый диск из списка подключенных дисков и нажать клавишу «Enter». На появившейся форме в разделе [Действия], выбрать пункт - <Установить защиту>;

– затем в разделе [Установить защиту] выбрать <тип пароля> и <security level>, внимательно читая советы-подсказки в правой части экрана. Сначала для User-пароля, затем для Master-пароля. Пароли устанавливаются с последующим подтверждением. Поддерживаются пароли до 32 символов;

– обязательно сохранить эти пароли на любом доступном носителе в надежном месте.

***Примечание**. Необходимо тщательно хранить пароль на диск. В случае потери паролей можно потерять всю информацию на диске. Снятием блокировок в случае утраты Master-пароля занимаются узкоспециализированные сервисы!*

После установки пароля появится информационное сообщение:

«Для того, чтобы изменения вступили в силу необходимо выключение питания».

После включения на экране будет появляться окно запроса:

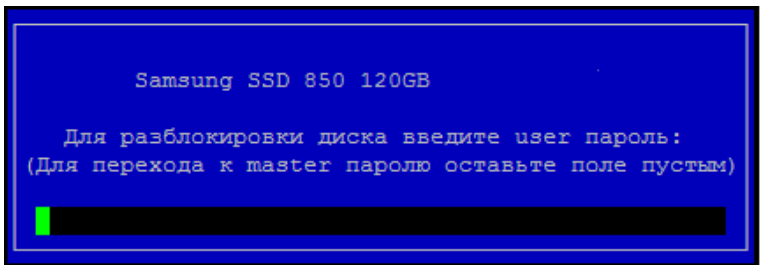

Рисунок 50 – Окно запроса пароля для жесткого диска

Окно запроса будет выводиться во время загрузки прогресс-бара инициализации БСВВ и появления окна «Главного меню».

Если установлены несколько жестких дисков с контролем доступа, то будут последовательно выведены формы запросов паролей для каждого диска.

Если пароль не введен, диск будет недоступен для использования, в меню контроля доступа будут активны чекбоксы для параметров <Security Enabled> и <Security locked>.

При корректном вводе пароля – только <Security Enabled>.

При вводе некорректного пароля дважды, происходит блокировка и заполняется поля: <Security Count Expired>, <Security Locked>(см.рисунок 51).

Значения сбрасываются при отключении питания. На экран выводится сообщение об ошибке:

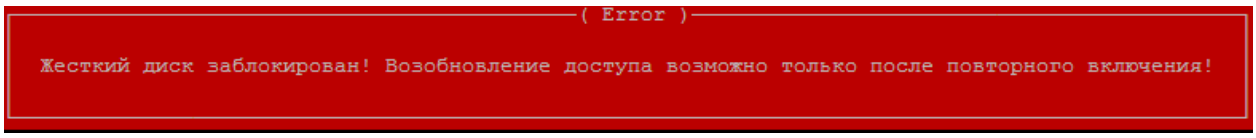

Рисунок 51 – Окно сообщения об ошибке

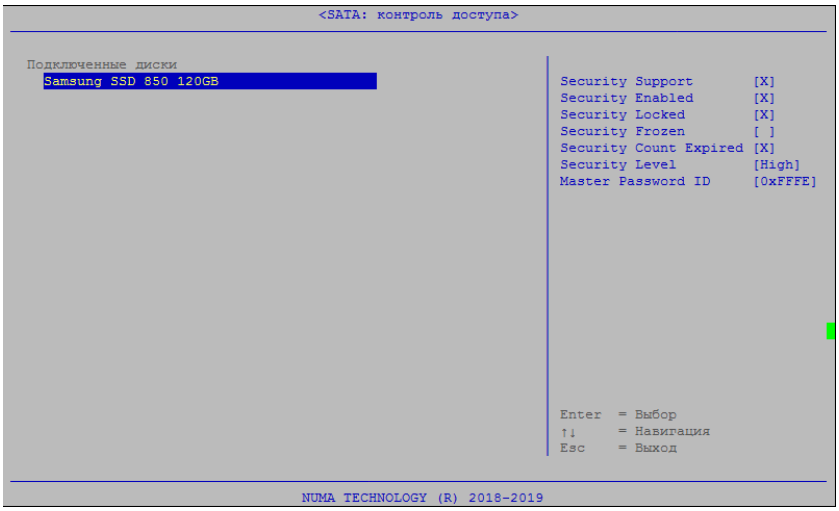

Рисунок 52 – Состояния полей формы контроль доступа при блокировке диска

При попытке выполнить какие-либо действия на форме контроля доступа, БСВВ выведет следующее сообщение:

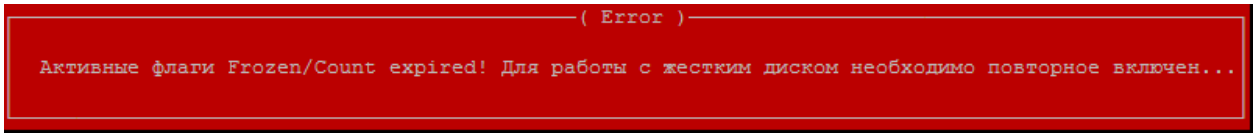

Рисунок 53 – Сообщение на форме контроля доступа

Поле <Security Frozen> заполняется, если после ввода пароля и загрузки ОС выполнить перезагрузку. Перезагрузка происходит без запроса пароля к диску. Загрузка ОС в этом случае разрешена.

Для снятия защиты необходимо:

– выбрать жесткий диск с установленной защитой и нажать клавишу «Enter»;

– на появившейся форме в разделе [Действия], выбрать пункт- <Снять защиту>;

– ввести значение User-пароля в диалоговой форме – «Введите старый пароль». После ввода корректного пароля, появится сообщение – «Операция выполнена»;

– вернуться на форму с разделом [Подключенные диски] и убедиться, что для диска активен только один чекбокс – <SecuritySupport>.

5.6.3.12. MISC: настройка BMC

Для настройки удаленного подключения к BMC-контроллеру необходимо перейти в меню «Драйверы устройств», выбрать раздел «MISC: настройка BMC».

Для работы можно выбрать динамическое назначение IP-адреса, для этого необходимо включить параметр DHCP или задать статический IP-адрес, указав дополнительно маску подсети и адрес шлюза. Для внесения изменений необходимо сохранить введенные данные.

Дальнейшее подключение к Изделию осуществляется через браузер на управляющем компьютере.

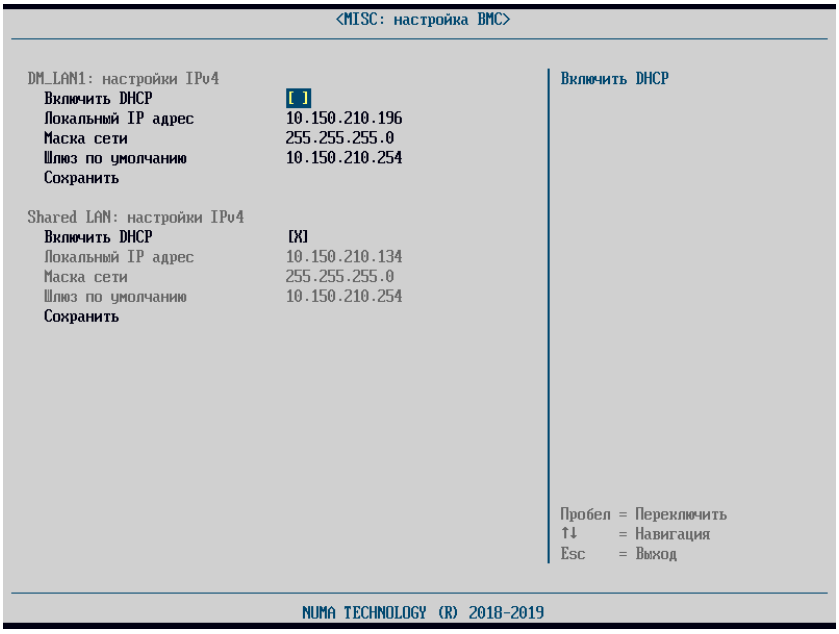

Рисунок 54 – MISC: настройка BMC. Задание статических настроек узла сети

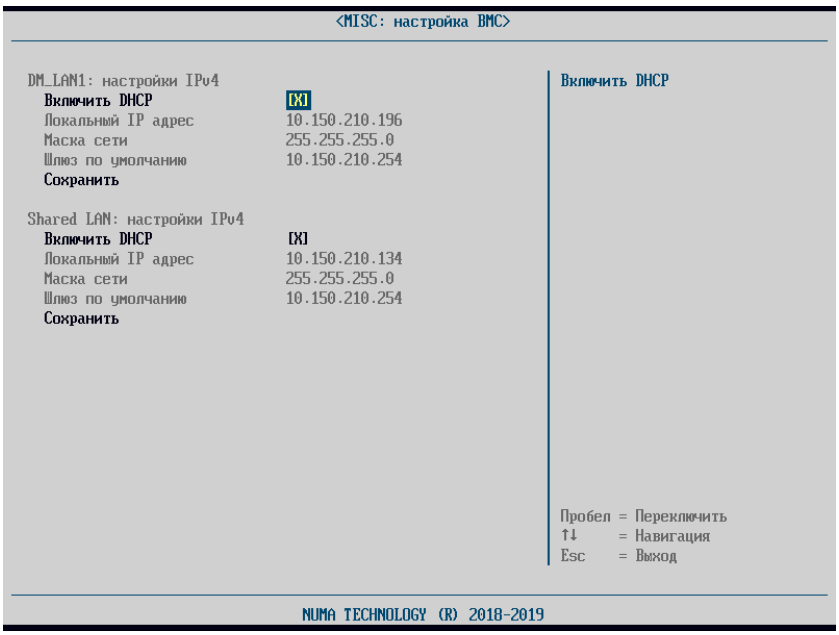

Рисунок 55 – MISC: настройка BMC. DHCP

5.6.3.13. PCI: конфигурация

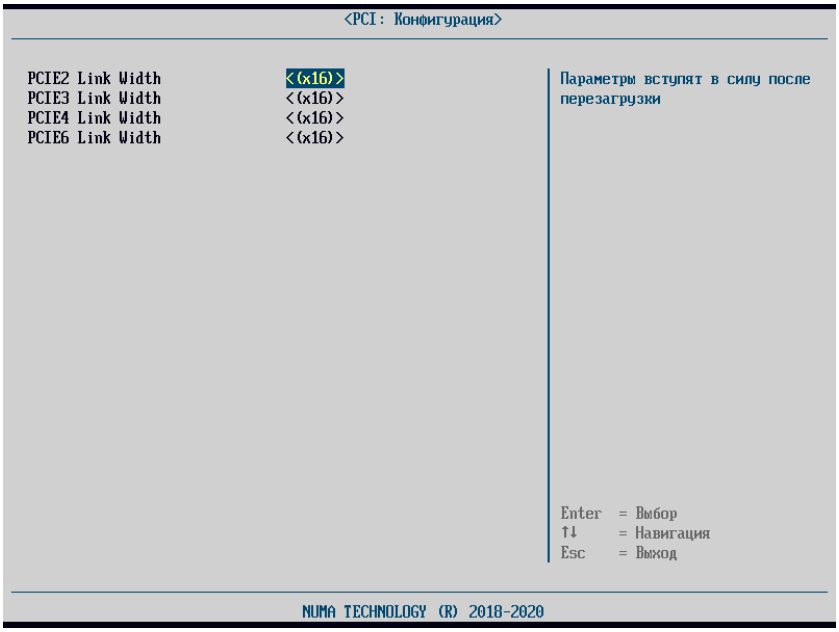

Рисунок 56 – Форма меню «PCI конфигурация»

Данная настройка позволяет устанавливать количество используемых линий шины PCIe для соответствующего порта.

Для выбора необходимого параметра необходимо нажать клавишу «Enter» и клавишами навигации выбрать подходящее значение.

Примечание. *Выбранные параметры вступят в силу только после перезагрузки!*

5.6.3.14. LAN: настройка Bypass

Данный пункт меню позволяет настраивать режим Bypass. Поддерживаются следующие варианты конфигурации интерфейсов: LAN1/LAN2 и LAN3/LAN4.

В режиме Bypass порты LAN1 и LAN2 (LAN3 и LAN4) напрямую замыкаются друг с

другом, сетевой трафик идет напрямую между портами и не попадает на сетевые интерфейсы.

При активном переключателе порты находятся в режиме Bypass. При неактивном переключателе порты функционируют как обычные порты Ethernet.

Настройка портов при включении (параметры в разделе «Питание ВКЛ») определяет поведение Bypass при работе в Numa Arce и в ОС.

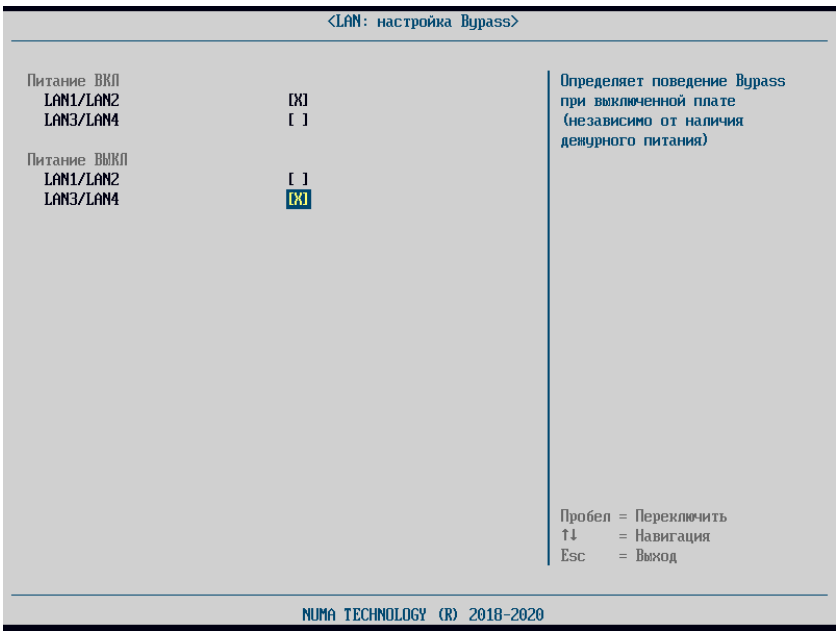

Рисунок 57 – Форма меню LAN:bypass

5.6.3.15. TPM 2.0: конфигурация

Данный пункт позволяет администратору включить/отключить поддержку TPM 2.0 для конфигурации Intel PTT с помощью механизма чекбоксов (см. рисунок 58).

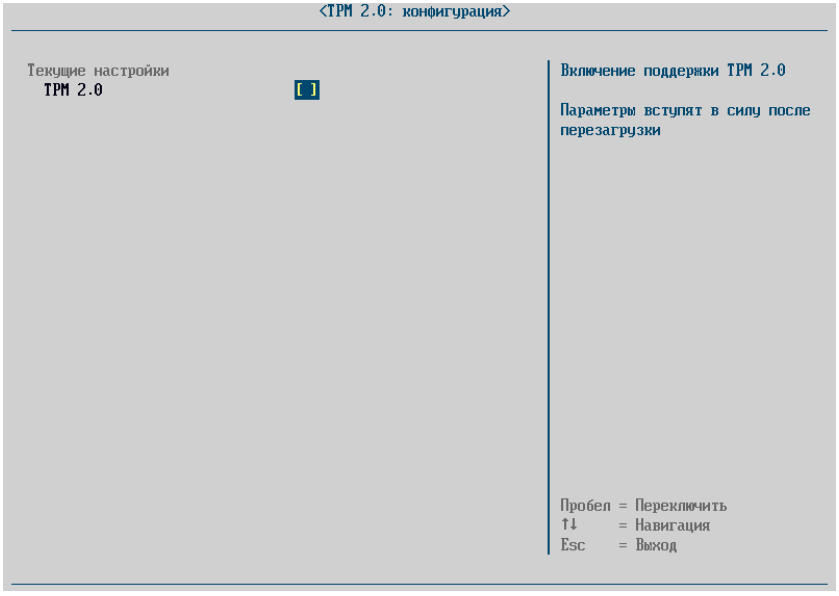

Рисунок 58 – Настраиваемый параметр поддержки TPM 2.0

***Примечание**. Для того чтобы изменения вступили в силу обязательно выполните перезагрузку!*

5.6.3.16. CPU: управление питанием

Данный параметр позволяет задать ограничение мощности процессора (см. рисунок 59).

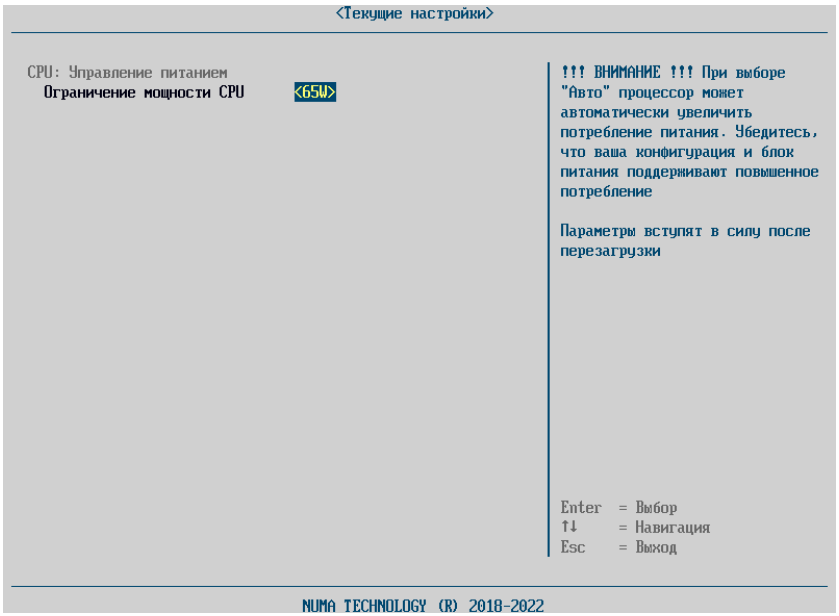

Рисунок 59 – Меню «CPU: управление питанием»

Доступно 4 значения энергопотребления процессора:

– 35W;

– 65W;

– 95W;

– Авто.

Внимание! При выборе значения «Авто» процессор может автоматически увеличить потребление питания. Убедитесь, что ваша конфигурация и блок питания поддерживают повышенное потребление.

***Примечание**. Для того чтобы изменения параметров вступили в силу обязательно выполните перезагрузку!*

5.7. Раздел «Параметры МДЗ»

5.7.1. «Пользователи»

Операции управления пользователями Изделия осуществляются из основного пункта меню «Пользователи», которое содержит три раздела: «Профили пользователей», «Действия с пользователями», «Настройка» (см. рисунок 60). Раздел «Действия с пользователями» следующие пункты:

– скачивать с LDAP;

– создать пользователя;

– сохранить на USB.

Раздел «Настройка» содержит пункты:

– политика паролей;

– управление токеном.

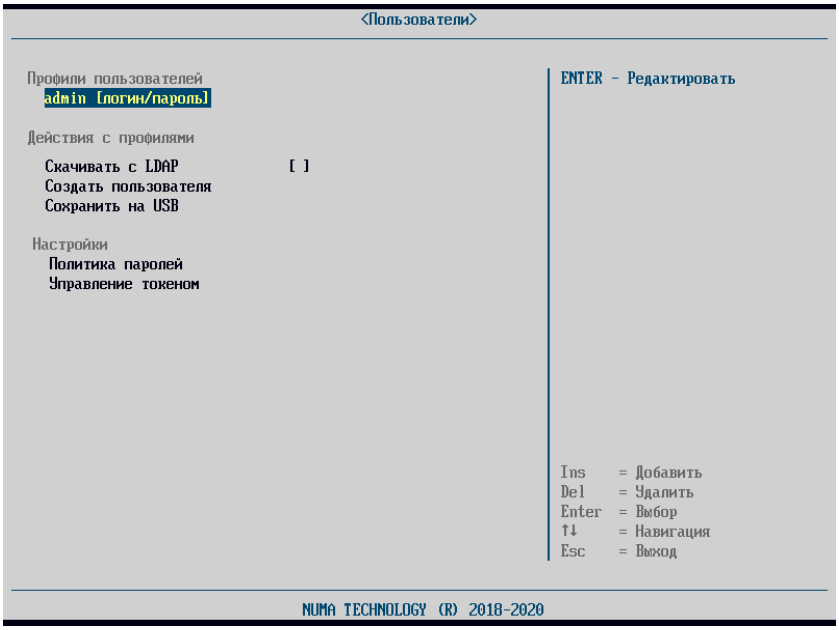

Рисунок 60 –Пункты меню «Управление пользователями»

5.7.1.1. Создание профиля пользователя

Для создания пользователя необходимо выполнить следующие действия (см. рисунок 64):

– выбрать пункт меню «Создать пользователя» или нажать клавишу «Ins»;

– заполнить атрибуты пользователя:

а) «Тип авторизации» – «логин/пароль», «АНП» или сочетание «АНП + логин/пароль»;

***Примечание**. Для создания пользователя с типом авторизации «АНП» или «АНП+логин/пароль» необходим токен, который можно проинициализировать в меню «Управление токеном» (см. раздел 5.7.1.5), или уже проинициализированный токен с загруженными корневыми сертификатами в соответствующий раздел меню (см. раздел 5.7.2).*

б) «Тип пользователя» – «Пользователь/Администратор»;

в) «Имя пользователя» – задать в окне ввода данных имя пользователя (логин). Текущие ограничения на имя пользователя: не менее 3 символов и не более 25 символов;

***Примечание.** Изделие не чувствительно к регистру вводимых символов имени пользователя (логина). Например, Admin, admin и AdMiN являются равнозначными.*

г) «Ф.И.О. пользователя»;

д) «Контактная информация»;

– для пользователей типа «Администратор» выбрать значение поля «Роль администратора». Доступны значения «Полный доступ» или «Аудит»;

Примечание. *Рекомендуется добавлять не более одного Администратора и не присваивать право «Полный доступ» без необходимости.*

– для пользователя с типом авторизации «АНП» или «АНП+логин/пароль» (пример см. рисунок 64) требуется задать следующие поля:

– «Тип сопоставления» – установить флаг для полей, по которым будет осуществляться сопоставление сертификата на АНП (CN, MAIL, DIGEST). Рекомендуется всегда устанавливать флаг на поле DIGEST, так как в отличие от других полей оно уникально, что позволит корректно создать пользователя с типом авторизации «АНП» или «АНП+логин/пароль»;

– «Данные сопоставления» – могут быть заданы из текстового файла с внешнего USB–носителя или с АНП. Для того чтобы ввести данные сопоставления с внешнего USB–носителя, необходимо выбрать пункт меню «Данные сопоставления» и выбрать файл с данными (см. рисунки 61 и 62).

При выборе корневого сертификата в роли данных сопоставления Изделие выдаст ошибку (см. рисунок 63).

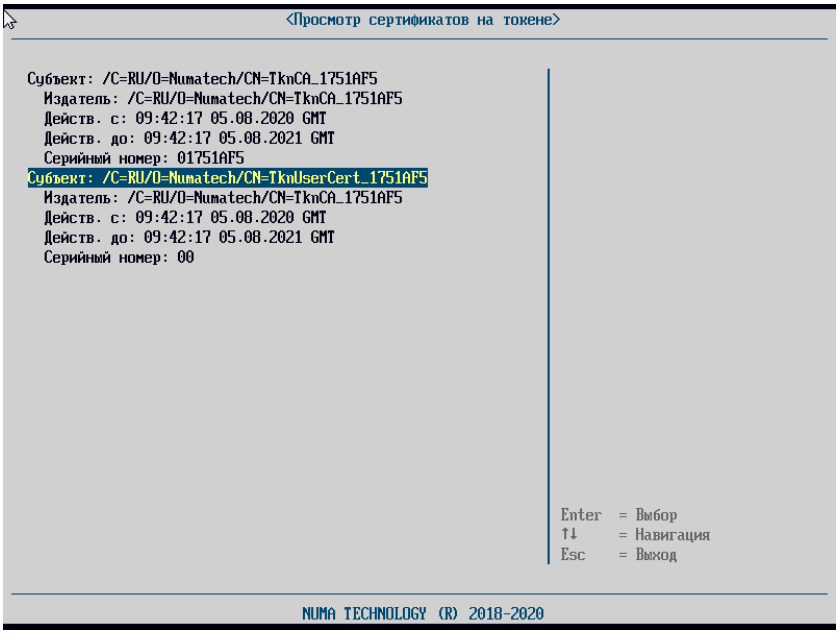

Рисунок 61 – Просмотр сертификатов на токене

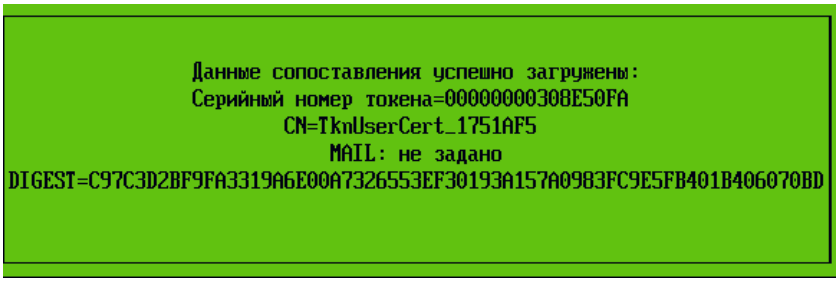

Рисунок 62 – Данные для сопоставления

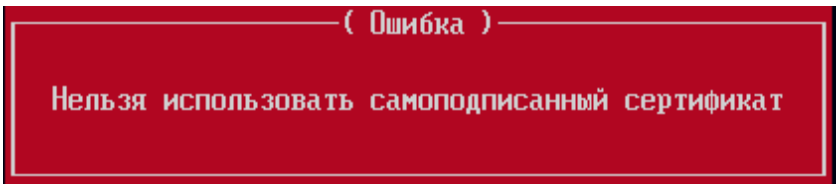

Рисунок 63 – Использование неверного сертификата

Данные для сопоставления необходимо задать согласно типу следующим образом:

– CN (Common Name) – согласно стандарту X.509 в следующем формате: /C= <код страны, RU>/ST = <кодсубъекта>/L = <Город>/O = <Имя организации>/OU = <Имя подразделения>/CN = <Имя пользователя>/emailAddress = <адрес электронной почты>;

– MAIL – по полному адресу электронной почты формата <username>@<domain.fqdn>;

– DIGEST – подпись X.509-сертификата – в формате 16-ричного числа, в форме <байт_0>:<байт_1>: … :<байт_n>;

– «Тип сопоставления». Рекомендуется всегда устанавливать флаг на поле DIGEST, так как в отличие от других полей оно уникально, что позволит корректно создать пользователя с типом авторизации «АНП».

– сохранить изменения, выбрав пункт меню «Создать».

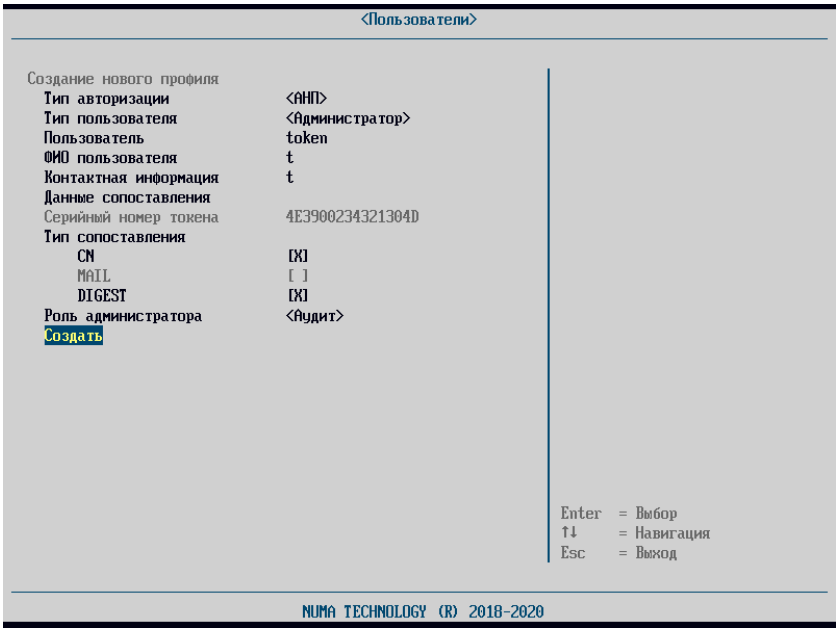

Рисунок 64 – Пример заполнения карточки пользователя с типом авторизации «АНП»

Для создания дистанционно назначенных списков пользователей следует:

– в разделе меню «Дополнительные настройки» ввести дополнительные настойки для LDAP;

– перейти в меню «Управление пользователями»;

– выставить флаг «Скачивать с LDAP» (см. рисунок 65);

– перезагрузить комплекс – после перезагрузки появится список пользователей, созданных на сервере LDAP.

Примечание. *При скачивании списка пользователей с сервера, локально созданные пользователи будут заменены пользователями с сервера LDAP.*

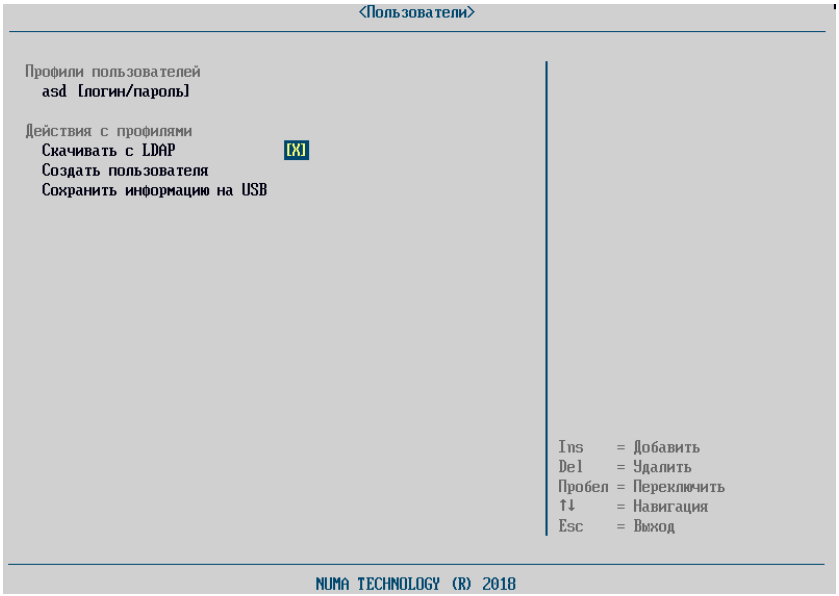

Рисунок 65 – Установка признака «Скачивать с LDAP»

Если при заполнении карточки пользователя указаны не все атрибуты, то Изделие выдаст сообщение об ошибке и укажет поля, обязательные к заполнению.

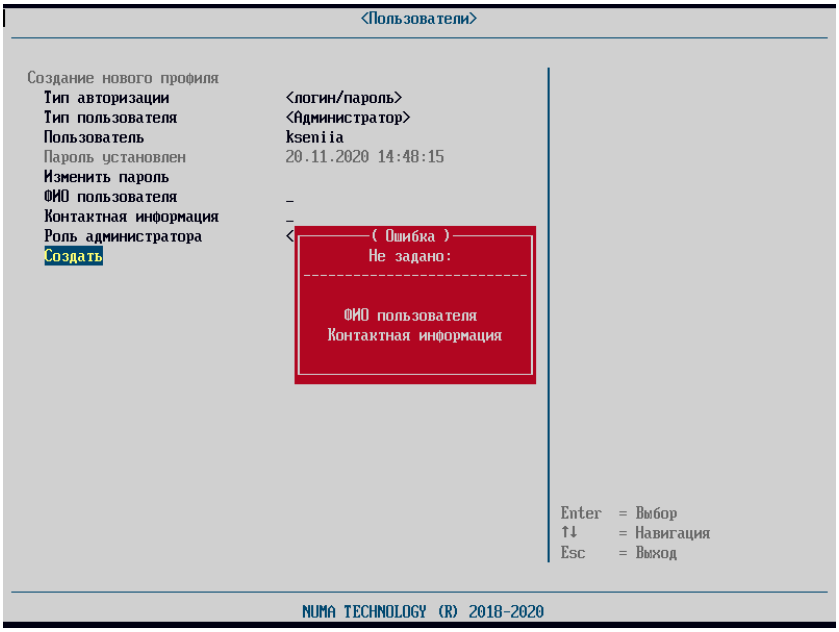

Рисунок 66 – Ошибки создания пользователей

При вводе логина уже существующего пользователя Изделие также выдаст сообщение об ошибке и не создаст пользователя (см. рисунок 67).

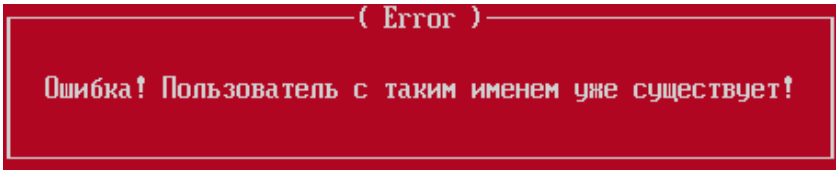

Рисунок 67 – Сообщение об ошибке при создании пользователя

При вводе пароля, не соответствующего действующей парольной политике, Изделие выдаст сообщение об ошибке и не позволит установить набранный пароль.

***Примечание**. Информацию о парольной политике смотрите в разделе 5.7.1.4.*

5.7.1.2. Просмотр/редактирование/удаление профиля пользователя

Для просмотра/редактирования пользователей необходимо выполнить следующие действия:

– выбрать в подменю «Профиль пользователя» пользователя, чьи данные необходимо просмотреть или отредактировать;

– изменить/просмотреть необходимые данные;

– выбрать пункт «Обновить» для сохранения внесенных изменений или нажать клавишу «Esc» для выхода без сохранения.

***Примечание**. При изменении пароля новый вариант необходимо будет ввести повторно для подтверждения. Если второй раз при вводе будет допущена ошибка, об этом будет выдано предупреждение. Пароль в этом случае заменён не будет.*

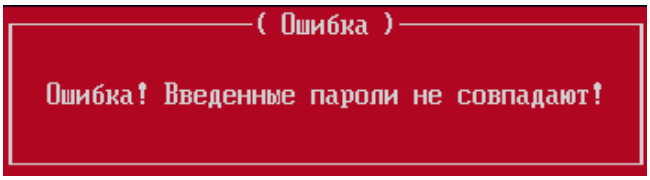

Рисунок 68 – Ошибка ввода пароля

При успешном сохранении изменений будет выведено сообщение:

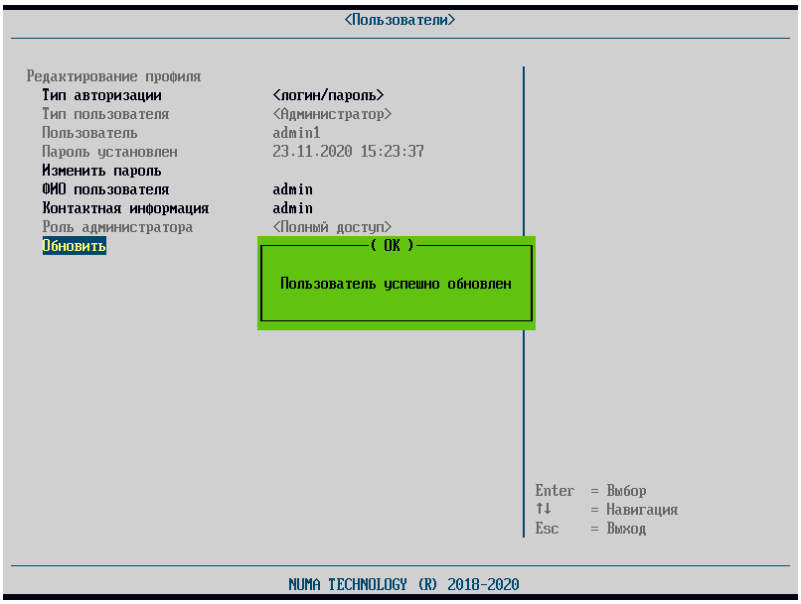

Рисунок 69 – Успешное обновление пользовательской информации

Если изменению подверглась текущая запись администратора, система автоматически будет перезагружена для применения новых значений параметров после предупреждения:

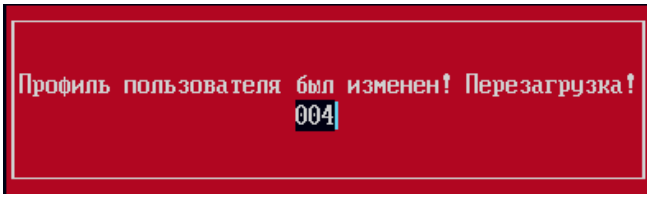

Рисунок 70 – Перезагрузка текущего профиля после успешной процедуры изменения пользовательской информации

Для удаления пользователя необходимо выполнить следующие действия:

– выбрать пользователя, которого необходимо удалить и нажать клавишу «Del»;

– в диалоге запроса на подтверждение удаления выбрать клавишу «Y» для удаления пользователя или клавишу «N» для отмены (см. рисунок 71).

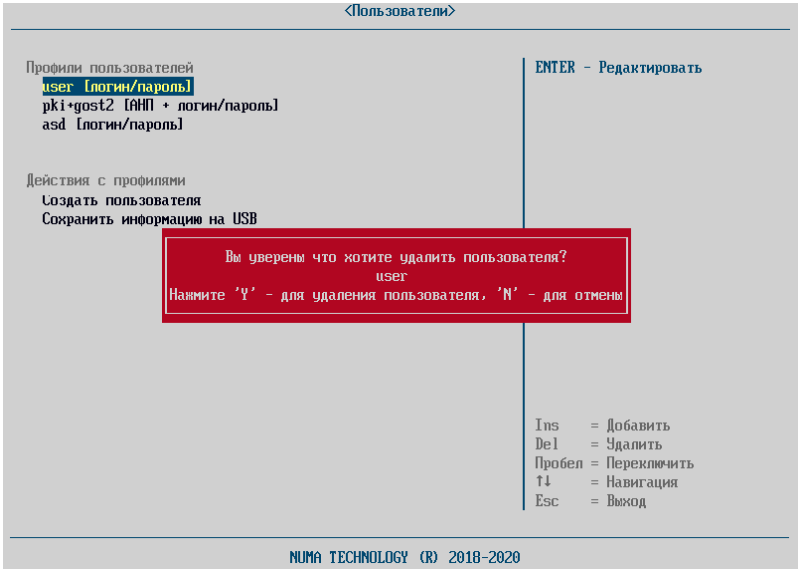

Рисунок 71 – Вид операции подтверждения удаления пользователя

Примечание. *Перед процедурой удаления пользователя необходимо выгрузить и очистить журнал аудита. В автоматическом режиме в журнал добавятся уведомления о том как и когда выгрузил и очистил журнал аудита.*

5.7.1.3. Экспорт профилей пользователей

Для сохранения данных пользователей на USB-носитель необходимо выполнить следующие действия:

– подключить USB–носитель;

– выбрать пункт меню «Сохранить информацию на USB». В случае успешного сохранения данных на экране появится сообщение:

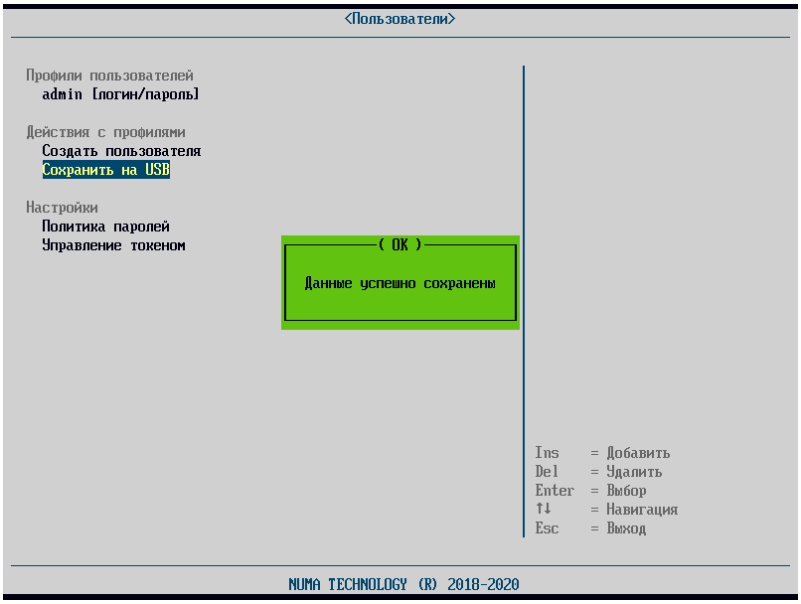

Рисунок 72 – Сообщение об успешном экспорте профилей пользователей

Примечание. *При ошибке экспорта профилей пользователей на USB-накопитель необходимо проверить тип файловой системы USB-накопителя.*

5.7.1.4. Политика паролей

Изделие поддерживает настраиваемую парольную политику. Для настройки парольной политики необходимо перейти в меню «Пользователи» → «Политика паролей» (см. рисунок 73).

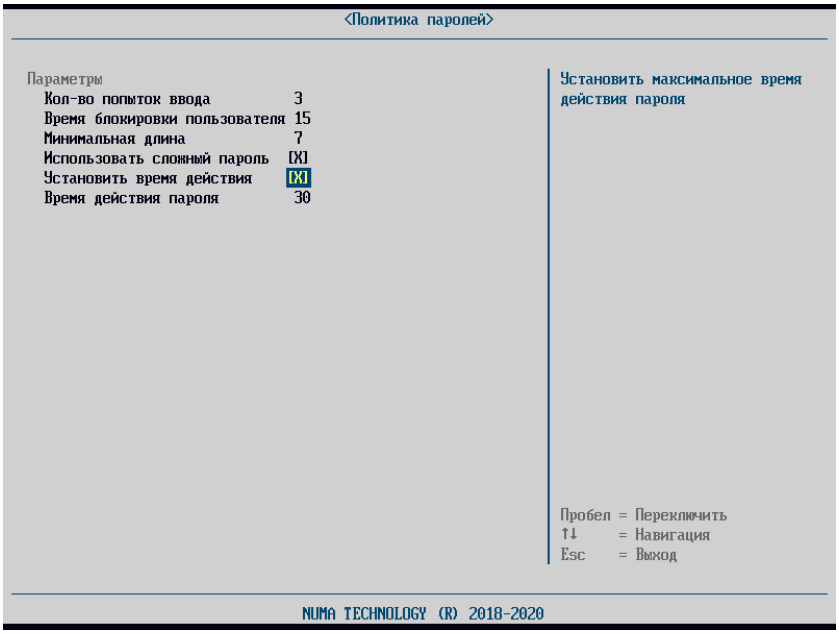

Рисунок 73 – Меню настройки парольной политики

«Количество попыток входа» – данный параметр указывает на количество неуспешных попыток аутентификации пользователя (только для ввода пароля при типе авторизации АНП+логин/пароль или логин+пароль). Параметр может принимать значения от 1 до 8. При превышении числового параметра, учетная запись пользователя блокируется на время, установленное в параметре «Время блокировки».

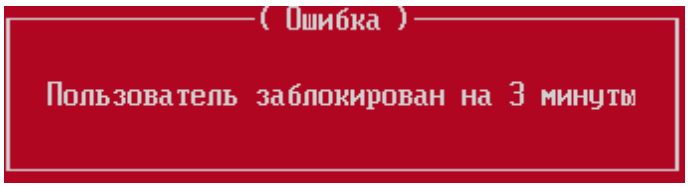

Рисунок 74 – Сообщение о блокировании пользователя

Для изменения числового параметра необходимо нажать клавишу «Enter» и ввести числовой параметр. При попытке ввода числового параметра отличного от 1 или 8, Изделие автоматически установит значение числового параметра равного 3.

Максимальное количество неуспешных попыток аутентификации при типе авторизации АНП задается в АНП вне Numa Arce. В случае ввода неверного ПИН-кода Изделие выдает ошибку (см. рисунок 75).

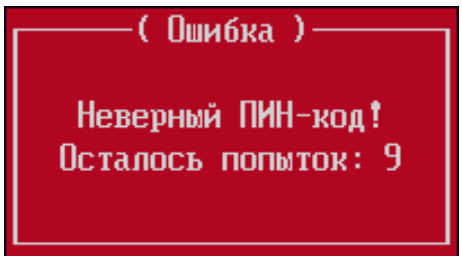

Рисунок 75 – Ошибка ввода ПИН-кода токена

«Время блокировки пользователя» – параметр регламентирует время блокировки учетной записи пользователя при превышении неуспешных попыток аутентификации.

Числовой параметр времени блокировки может принимать значения от 3 минут до 60 минут.

Для изменения числового параметра необходимо нажать клавишу «Enter» и ввести числовой параметр. При попытке ввода числового параметра отличного от допустимого, Изделие автоматически установит значение числового параметра равного 3.

«Минимальная длина» – параметр, указывающий минимально допустимую длину пароля пользователя. Числовой параметр, устанавливающий длину пароля, находится в диапазоне от 1 до 20 символов.

Для изменения числового параметра необходимо нажать клавишу «Enter» и ввести числовой параметр. При попытке ввода числового параметра отличного от допустимого, Изделие автоматически установит значение числового параметра равного 7.

«Сложность пароля» – при включении данного параметра в пароле должны использоваться символы не менее чем из 3 следующих категорий (алфавит пароля 75 символов):

- прописные буквы английского алфавита от 'A' до 'Z';
- строчные буквы английского алфавита от 'a' до 'z';
- десятичные цифры от 0 до 9;
- спецсимволы (~ ! @ # $ % ^ & * ( ) - + { } [ ] ; ' : " , < >).

При выключенном параметре «Использовать сложный пароль» ограничения не накладываются.

Для переключения параметра «Сложность пароля» в активное состояние необходимо нажать клавишу «Пробел».

«Установить время действия пароля» – параметр, отвечающий за срок действия пароля. При включении данного параметра в поле «Время действия пароля» устанавливается числовой параметр действия пароля. Числовой параметр может принимать значение от 30 до 365 дней.

По истечении срока действия пароля выводиться сообщение об истечении срока действия и необходимости смены пароля и блокируется возможность загрузки ОС.

При выключенном параметре «Установить время действия» ограничения на срок действия пароля не накладываются.

Для переключения параметра «Установить время действия» в активное состояние необходимо нажать клавишу «Пробел».

Для ввода действия пароля необходимо нажать клавишу «Enter» и ввести числовой параметр в диапазоне от 30 до 365. При попытке ввода числового параметра отличного от допустимого, Изделие автоматически установит значение числового параметра равного 30.

5.7.1.5. Управление токеном

5.7.1.5.1. Инициализация токена

Для инициализации токена в Изделии необходимо:

– авторизоваться под учетной записью администратора;

– вставить токен в USB-порт;

– перейти в меню «Пользователи» → «Управление токеном»;

– выбрать срок действия токена после инициализации (см. рисунок 76);

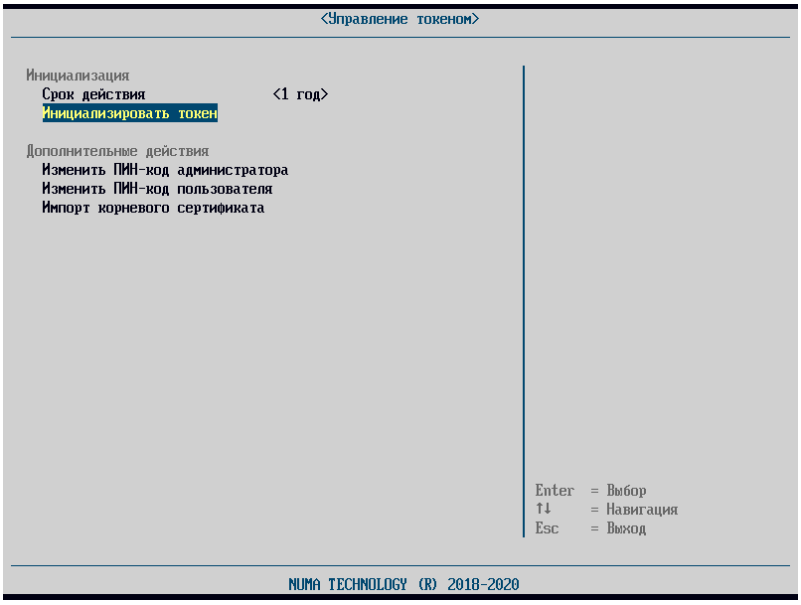

Рисунок 76 – Инициализация токена. Срок действия токена

– выбрать меню «Инициализировать токен». После инициализации предыдущие данные на токене будут удалены, необходимо подтвердить необходимость инициализации токена (см. рисунок 77)

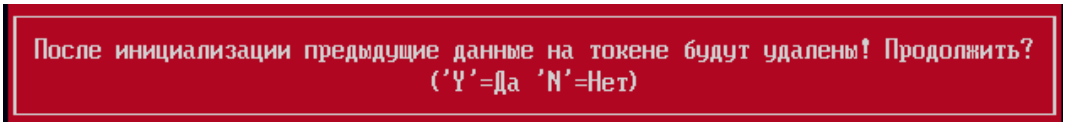

Рисунок 77 – Диалог подтверждения инициализации токена

– далее запустится процесс инициализации токена (см. рисунок 78),

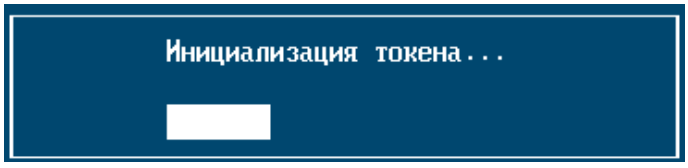

Рисунок 78 – Инициализация токена

– после успешной инициализации токена (см. рисунок 79) корневой сертификат данного токена автоматически будет добавлен в хранилище в меню «Сертификаты» (см. рисунок 80).

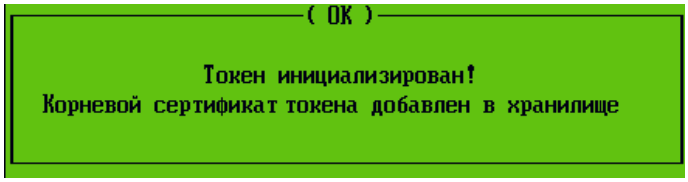

Рисунок 79 – Успешное завершение инициализации токена

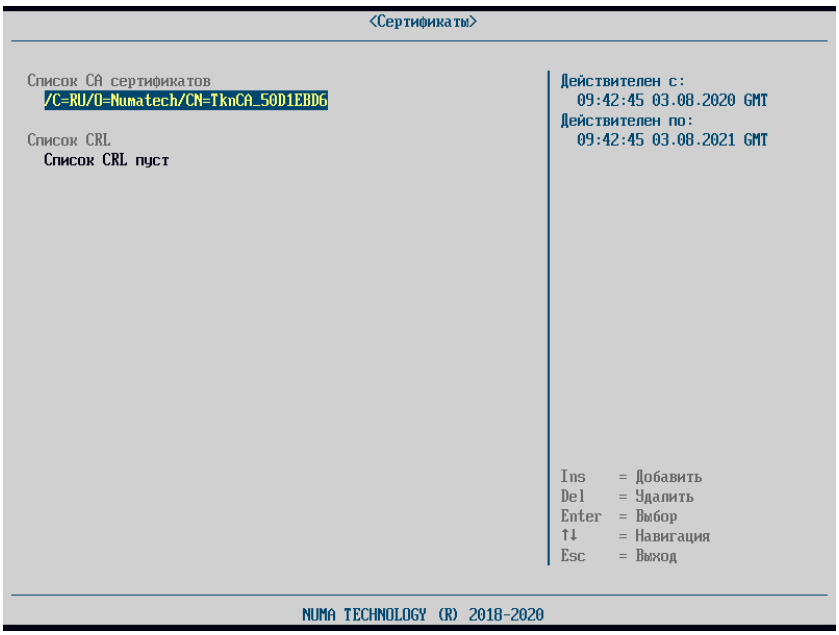

Рисунок 80 – Сертификаты. CA сертификат инициализированного токена

5.7.1.5.2. Изменение ПИН-кода токена

После инициализации токена необходимо изменить предустановленный ПИН-код токена.

Изменение ПИН-кода администратора и пользователя позволяет изменить ПИН-код как с использованием генератора паролей (используя ресурсы токена), так и вручную.

Для генерации нового ПИН-кода токена необходимо перейти в меню «Изменение ПИН-кода токена пользователя» или «Изменение ПИН-кода токена администратора». В отобразившемся окне выбрать необходимый метод генерации: «Вручную» – параметры задаются пользователем, «Сгенерировать» – генерация осуществляется за счет криптографических функций, реализованных на токене.

После выбранного метода Изделие запросит ПИН-код администратора токена. При первой инициализации токена ПИН-код администратора установлен по умолчанию. Актуальный ПИН-код администратора необходимо узнать из эксплуатационных документов на токен. В ином случае ПИН-код токена необходимо узнать у администратора безопасности предприятия.

После успешного ввода ПИН-кода администратора Изделие запросит новый пароль или сгенерирует пароль самостоятельно в зависимости от выбранного метода.

> ***Примечание.*** *Запомните ПИН-код токена для дальнейшей работы с ним.*

5.7.1.5.3. Импорт корневого сертификата

Для использования токена, который был инициализирован вне Изделия, необходимо импортировать корневой сертификат в Изделие. Для этого необходимо подключить токен, перейти в меню «Управление токеном» → «Импорт корневого сертификата». В появившемся списке выбрать корневой сертификат и нажать клавишу «Enter». Корневой сертификат автоматически будет импортирован в Изделие. Информацию о сертификате можно просмотреть в меню «Сертификаты» 5.7.2.

5.7.2. «Сертификаты»

Для управления сертификатами пользователей, а также сертификатов для загрузки ОС по сети необходимо выбрать пункт меню «Сертификаты».

5.7.2.1. Управление сертификатами пользователей

Доступны два варианта работы с сертификатами пользователей (для процедуры аутентификации): локальный и сетевой, через LDAP-сервер с TLS-сертификацией.

> ***Примечание**. При переключении с локального варианта работы на сетевой, все записи локальных пользователей будут удалены. Перед сменой режима работы необходимо сохранить профили пользователей, чтобы информация не пропала.*

Загрузка/обновления сертификата удостоверяющего центра поддерживается только с USB-носителя. Для загрузки сертификата необходимо выполнить следующие действия:

– подключить USB-носитель с сертификатом в СВТ;

– в меню «Сертификаты» перейти раздел «Список CA сертификатов»;

– нажать клавишу «Enter» или «Ins» и в запустившемся файловом обозревателе перейти в каталог, содержащий файл с цепочкой сертификатов удостоверяющего центра;

– выбрать файл цепочки сертификатов – будет выполнена загрузка сертификатов и в случае успешной загрузки/обновления цепочки сертификатов в строке меню будет прописано имя файла FILE_NAME, выбранного в качестве сертификата.

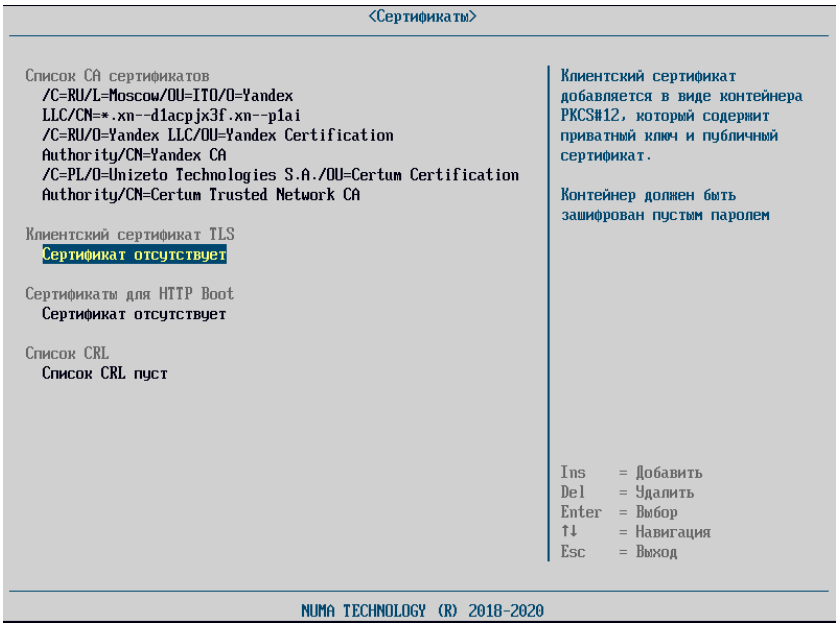

Рисунок 81 – Загрузка сертификата удостоверяющего центра

Для выполнения загрузки/обновления списка отозванных сертификатов необходимо выполнить следующие действия:

– выбрать пункт меню «Текущий CRL»;

– в файловом обозревателе выбрать файл, содержащий список отозванных сертификатов – в случае успешной загрузки/обновления сертификата в строке меню «CRL: <FILE_NAME>» будет прописано имя выбранного файла FILE_NAME.

Для выполнения загрузки/обновления сертификата удостоверяющего центра, подписавшего сертификаты TLS, необходимо выполнить следующие действия:

– подключить USB–носитель, содержащий файл сертификата, в СВТ;

– перейти в раздел «Список CA сертификатов»;

– нажать клавишу Enter или Ins и в запустившемся в файловом обозревателе

выбрать файл, содержащий сертификат УЦ – в случае успешной загрузки/обновления сертификата в строке меню будет прописано имя выбранного файла FILE_NAME.

Для выполнения загрузки/обновления клиентского сертификата TLS необходимо выполнить следующие действия:

– выбрать пункт меню «Клиентский сертификат TLS»;

– в файловом обозревателе выбрать файл, содержащий сертификат – в случае успешной загрузки/обновления сертификата, в меню «Текущий клиентский сертификат TLS» будет прописано имя выбранного файла FILE_NAME.

Для выполнения загрузки/обновления клиентского закрытого ключа TLS необходимо выполнить следующие действия:

– выбрать пункт меню «Текущий клиентский закрытый ключ TLS»;

– в файловом обозревателе выбрать файл, содержащий ключ – в случае успешной загрузки/обновления сертификата в строке меню «Текущий клиентский закрытый ключ TLS» будет прописано имя выбранного файла FILE_NAME.

Примечания:

В случае если файл не является файлом цепочки сертификатов или формат цепочки не DER, будет выведено сообщение об ошибке:

```
Ошибка! Неизвестный формат PKCS7 цепочки CA!
```

Если загружаемый сертификат не подписан загруженным ранее сертификатом УЦ, то будет выведено сообщение об ошибке.

Если сертификат находится в загруженном списке отозванных сертификатов, то будет выведено сообщение:

```
Сертификат отозван!
```

Если срок действия загружаемого сертификата еще не наступил, будет выдано сообщение:

```
Сертификат еще не вступил в действие
```

Для удаления цепочки сертификатов, CLR, клиентского сертификата TLS или клиентского закрытого ключа TLS необходимо выбрать соответствующий пункт меню и нажать клавишу Del.

5.7.2.2. Сертификаты для загрузки ОС по технологии HTTP Boot

Для загрузки ОС по технологии HTTP Boot необходимо подготовить загружаемый образ ОС, а также корневой сертификат удостоверяющего центра, сертификат администратора безопасности, подписавшего образ загрузки. Пример построения удостоверяющего центра и инфраструктуры открытых ключей, а также процесс подписи загружаемого образа с генерацией всех необходимых для загрузки элементов приведен в Приложении 5.

5.7.2.2.1. Загрузка/обновление корневого сертификата удостоверяющего центра

Для работы с загрузкой типа HTTP Boot необходимо загрузить корневой сертификат удостоверяющего центра. Изделие поддерживает PEM и DER форматы сертификатов.

Изделие поддерживает только локальную загрузку корневого сертификата удостоверяющего центра.

Для загрузки корневого сертификата удостоверяющего центра в Изделие необходимо:

– установить USB-накопитель в СВТ, на которое установлено Изделие;

– выбрать в разделе «Управление внутренними сертификатами», пункт меню «Текущая цепочка СА»;

– нажать клавишу «Enter» или «Ins», в запустившемся файловом обозревателе перейти в каталог, содержащий файл с корневым сертификатом удостоверяющего центра;

– выбрать файл корневого сертификата – будет выполнена загрузка сертификата и в случае успешной загрузки/обновления цепочки сертификатов в строке меню «Текущая цепочка СА: <FILE_NAME>» будет прописано имя файла FILE_NAME, выбранного в качестве сертификата.

После загрузки корневого сертификата удостоверяющего центра отобразится раздел «Сертификаты для HTTP Boot».

5.7.2.2.2. Загрузка/обновление сертификата администратора безопасности

Сертификат администратора безопасности, подписавшего образ ОС, который должен быть загружен с помощью технологии HTTP Boot, может быть загружен локально в отобразившемся разделе меню, для этого необходимо:

– установить USB-накопитель в СВТ, на которое установлено Изделие;

– перейти в раздел «Сертификаты для HTTP Boot»;

– нажать клавишу «Enter» или «Ins», в запустившемся файловом обозревателе перейти в каталог, содержащий файл сертификата;

– выбрать необходимый файл сертификата;

– после выбора сертификата наименование сертификата отобразится в разделе «Сертификат для HTTP Boot». При навигации в информационном блоке справа отображается срок действия сертификата (см. рисунок 82).

Также данный сертификат администратора безопасности можно разместить на сервере, где будет расположен загружаемый образ ОС.

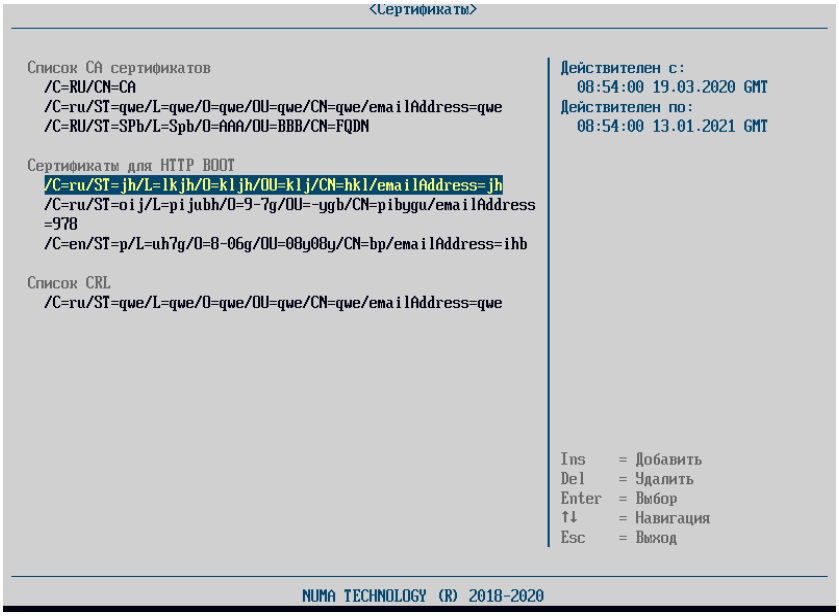

Рисунок 82 – Раздел сертификаты с указанными сертификатами для HTTP Boot

***Примечание**. Загружаемый сертификат администратора безопасности также должен быть подписан корневым сертификатом.*

5.7.2.2.3. Загрузка/обновление списка отозванных сертификатов удостоверяющего центра

Для выполнения загрузки/обновления списка отозванных сертификатов необходимо выполнить следующие действия:

– установить USB-накопитель в СВТ, на которое установлено Изделие;

– выбрать пункт «Текущий CRL»;

– в файловом обозревателе выбрать файл, содержащий список отозванных сертификатов – в случае успешной загрузки/обновления сертификата в строке меню «Текущий CRL: <FILE_NAME>» будет отображено имя выбранного файла FILE_NAME.

5.7.3. «Журнал аудита»

Управление журналом аудита осуществляется из пункта панели управления «Журнал аудита» (см. рисунок 83). Полный список регистрируемых событий приведен в Приложение 3.

После превышения максимального объема записей в разделах журнала работа Изделия блокируется. Для возобновления работы администратору необходимо выгрузить и очистить журнал аудита. В случае если настроена автоматическая перезапись (см. пункт 5.7.3.4), Изделие в автоматическом режиме перезаписывает записи аудита на новые при превышении объема раздела журнала аудита.

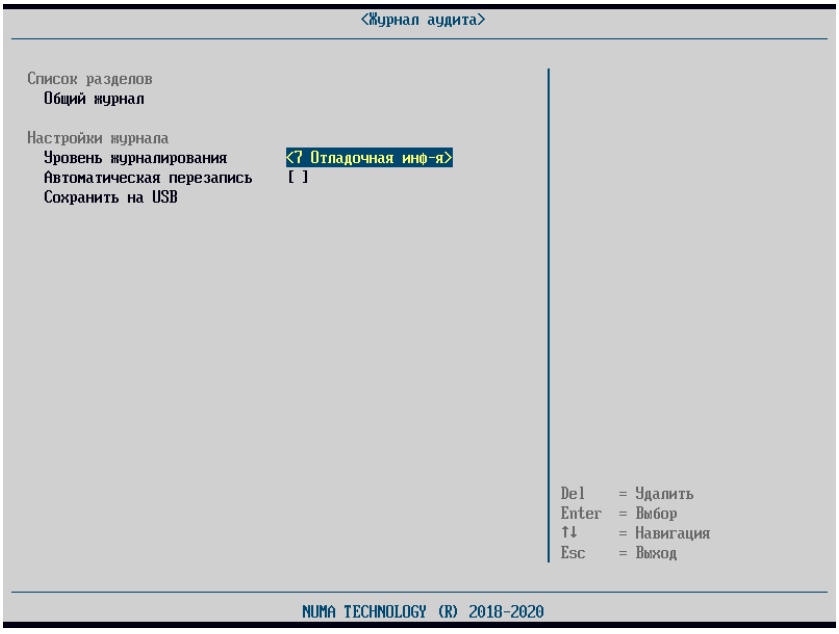

Рисунок 83 – Меню «Журнал аудита»

С записями в разделах журнала можно ознакомиться, выбрав пункт «Общий журнал». Записи имеют следующий формат (см. рисунок 84):

– время наступления события;

– имя пользователя, действиями которого инициировано событие;

– тип события;

– код события.

В поле подсказки отображаются:

– результат попытки осуществления действия (успешная или не успешная);

– описание события.

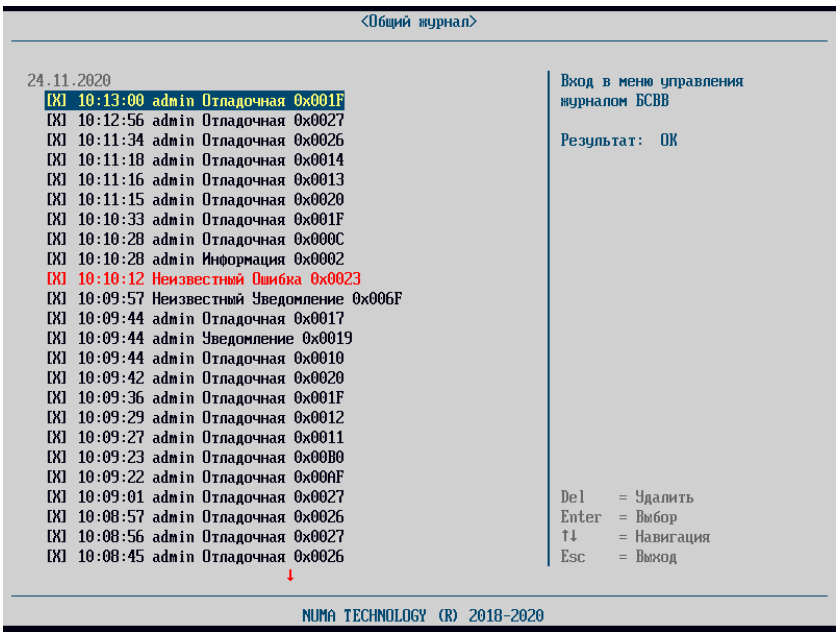

Рисунок 84 – Вид журнала аудита

5.7.3.1. Удаление записей из журнала аудита

Записи, ранее выгруженные на USB, отмечены [X] и доступны для удаления. Для удаления выделенной записи необходимо нажать «Enter». Если запись не была предварительно выгружена на USB-носитель, удаление будет заблокировано с выводом соответствующего сообщения (см. рисунок 85):

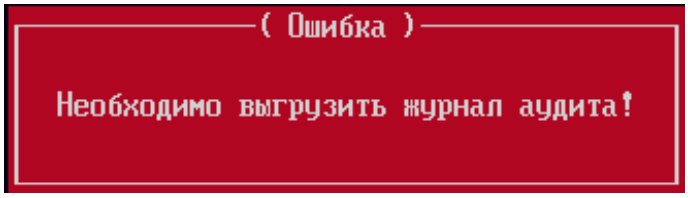

Рисунок 85 – Ошибка удаления невыгруженного журнала

Для удаления уже экспортированных данных (см. пункт 5.7.3.2) из Изделия необходимо подтвердить их удаление путем нажатия клавиши «Y», в случае отмены необходимо нажать клавишу «N», которая вернет в меню «Журнал аудита (см. рисунок 86).

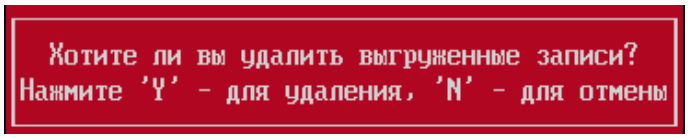

Рисунок 86 – Диалоговое окно удаление уже выгруженных данных

5.7.3.2. Экспорт журнала аудита

Для выгрузки журнала на внешний USB-носитель необходимо вставить USB-носитель в СВТ и выбрать пункт меню «Сохранить на USB».

В случае успешной выгрузки данных будет выдано сообщение:

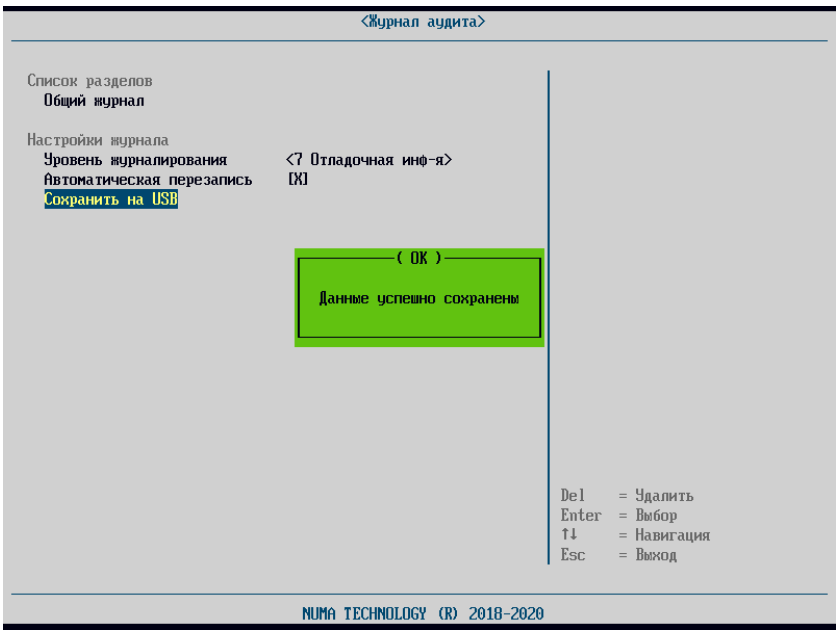

Рисунок 87 – Сообщение об успешном экспорте журнала аудита

В папке «\bios» появившейся на USB-носителе будет создан файл с записями истории Изделия. Имя файла создается автоматически по шаблону:

```
Journal[yy-mm-dd]
```

где `yy-mm-dd` – текущая дата.

Примечание. *Просмотр файла рекомендуется производить в программе «Notepad++».*

В случае отсутствия в USB-портах СВТ хотя бы одного рабочего носителя будет выдано сообщение об ошибке:

```
USB-носитель не найден!
```

Примечание. *При ошибке экспорта на USB-накопитель необходимо проверить тип файловой системы USB-накопителя.*

5.7.3.3. Уровень журналирования

В Изделии можно настраивать уровень критичности информации, которая будет записываться в журнал аудита. Уровень критичности может принимать следующие значения:

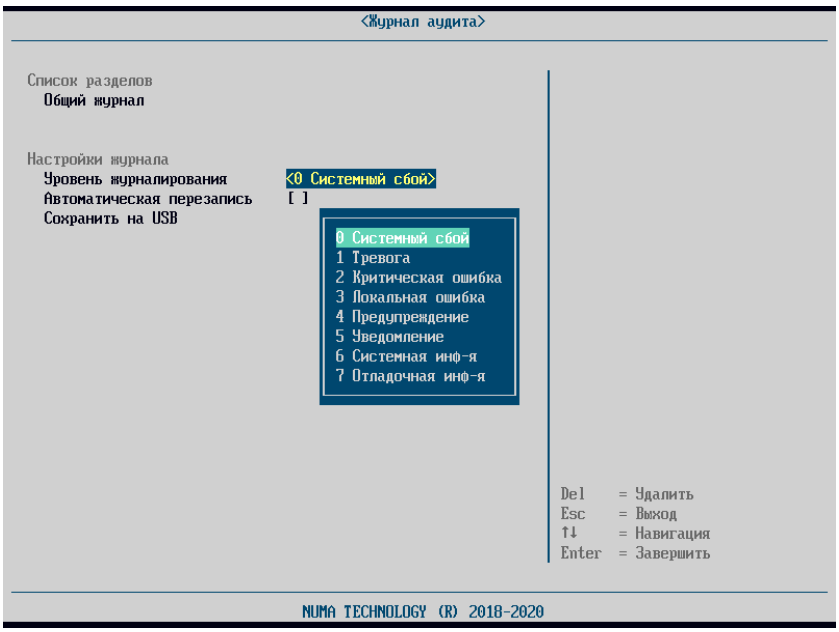

Рисунок 88 – Уровни журналирования

Для того чтобы задать уровень критичности событий, фиксируемых в журнале, необходимо выбрать пункт меню «Уровень журналирования» и задать значение уровня критичности из выпадающего списка.

5.7.3.4. Автоматическая перезапись

Для возможности автоматически перезаписывать невыгруженные записи при достижении предельного количества записей в журнале Изделия, можно включить функцию автоматической очистки. Для этого необходимо активировать пункт «Автоматическая перезапись».

5.7.4. «Параметры безопасности»

Раздел меню параметры безопасности предназначены для настроек безопасности загружаемых ОС (см. рисунок 89).

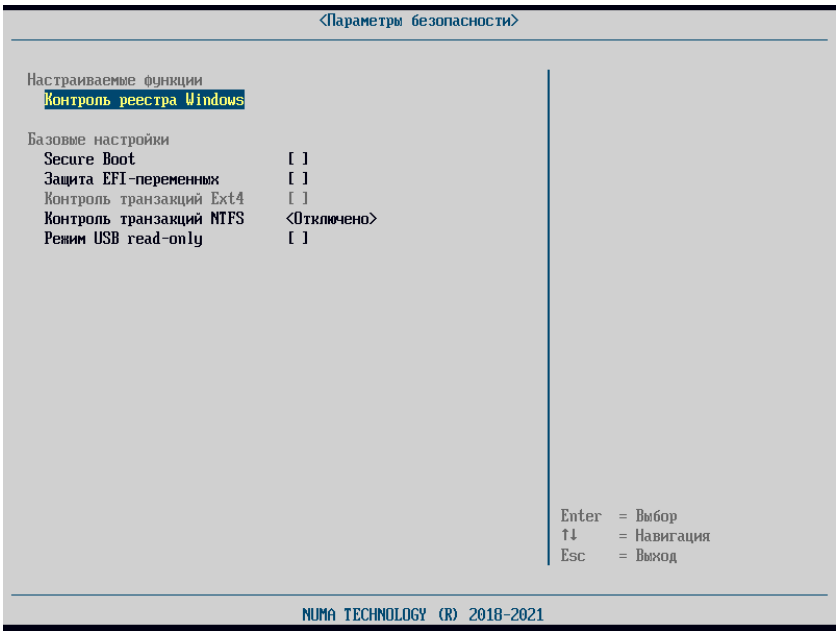

Рисунок 89 – Меню Параметры безопасности

5.7.4.1. Контроль реестра Windows

Раздел «Контроль реестра Windows» позволяет настраивать и просматривать контроль целостности элементов реестров Windows (см. рисунок 90).

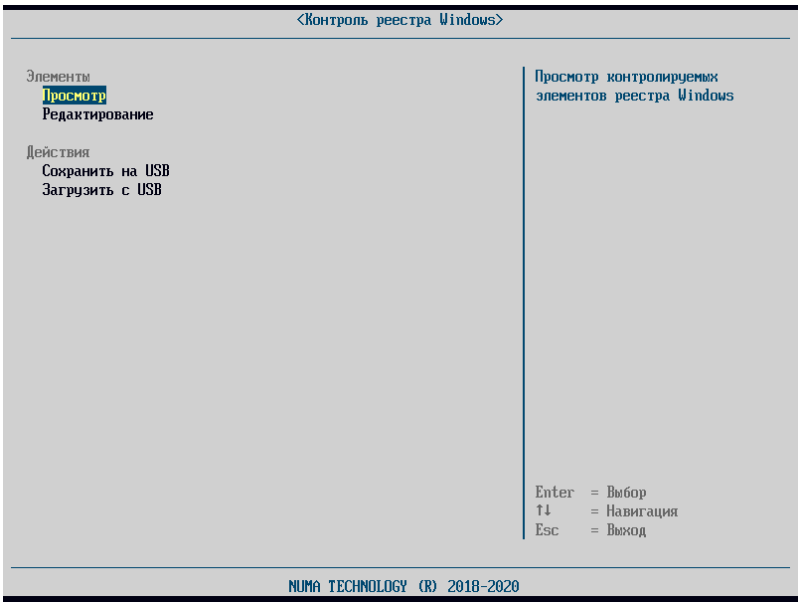

Рисунок 90 – Главное окно управления контролем целостности реестра Windows

5.7.4.1.1. Просмотр контроля целостности

Меню «Просмотр» позволяет выполнить просмотр контролируемых элементов реестра. На рисунке 91 представлено окно просмотра контролируемых элементов реестра Windows.

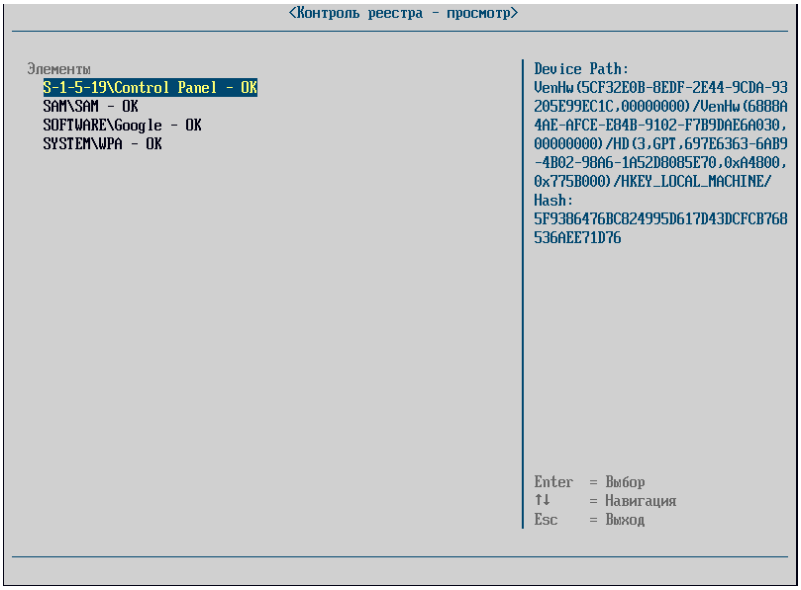

Рисунок 91 – Окно просмотра контролируемых элементов реестра Windows

При входе в меню просмотра у всех элементов, взятых на контроль, автоматически проверяется целостность. Если целостность хотя бы одного контролируемого элемента нарушена, то при переходе в меню «Просмотр» будет отображено сообщение об ошибке (см. рисунок 92). В конце имени элементов, целостность которых нарушена, добавляется строка «Ошибка».

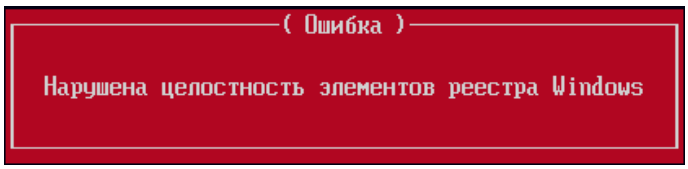

Рисунок 92 – Сообщение об ошибке при нарушении целостности элементов реестра Windows

5.7.4.1.2. Добавление элементов реестра в список контроля целостности

Меню «Редактирование» позволяет управлять списком контролируемых элементов реестра Windows. На рисунке 93 представлено окно редактирования элементов.

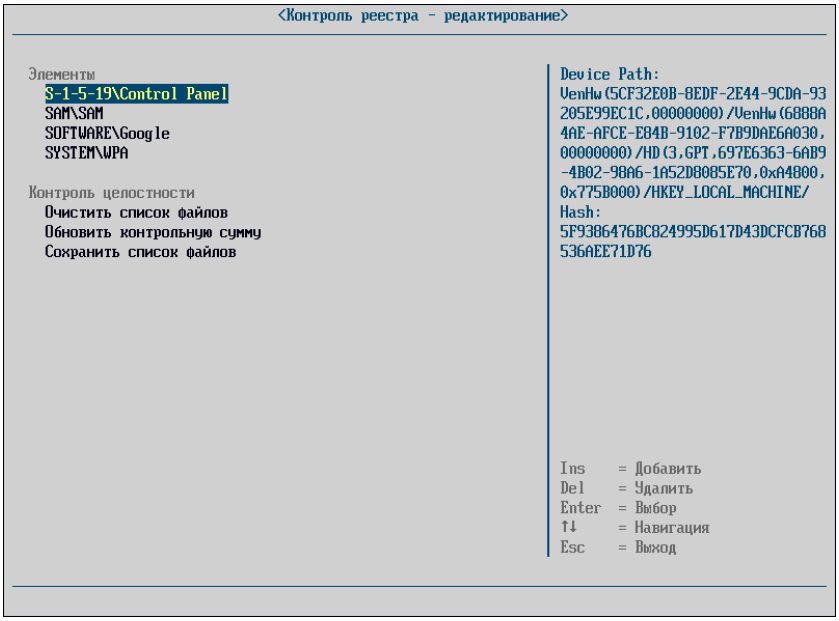

Рисунок 93 – Окно редактирования списка контролируемых элементов реестра Windows

Добавление разделов (каталогов) в список контроля целостности осуществляется путем нажатия клавиши «Insert». В окне файлового браузера отображается список разделов жесткого диска, содержащих реестр Windows.

В случае контроля каталога (раздела) реестра нарушение целостности наступает в следующих случаях:

– добавление/удаление файлов (параметров) из каталога, добавленного в список контроля целостности;

– модификация существующих файлов (параметров) в каталоге, добавленном в список контроля целостности.

Окно файлового браузера представлено на рисунке 94.

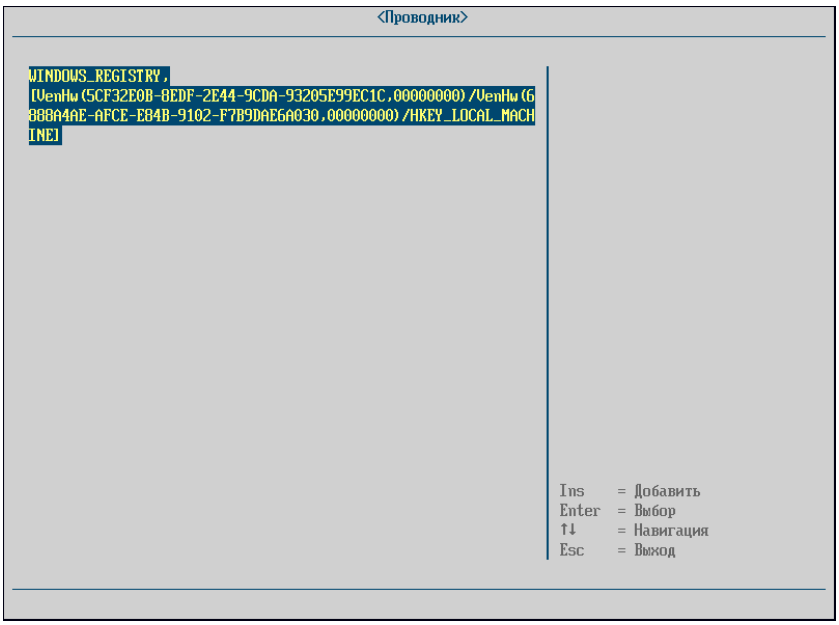

Рисунок 94 – Окно файлового браузера

Файловый браузер открывается только в том случае, если реестр Windows найден хотя бы на одном из разделов подключенных накопителей. Если реестр Windows отсутствует, выдается сообщение об ошибке:

«Файлы реестра Windows не найдены!».

После выбора устройства, содержащего реестр, становится доступен выбор разделов и параметров реестра для постановки их на контроль. Добавление файлов (параметров) реестра в список контроля целостности осуществляется путем нажатия клавиши «Enter». В случае если выбран каталог (раздел) реестра, то нажатие клавиши «Enter» приводит к отображению списка дочерних элементов (разделов и параметров) выбранного каталога.

Окно файлового браузера с разделами реестра представлено на рисунке 95.

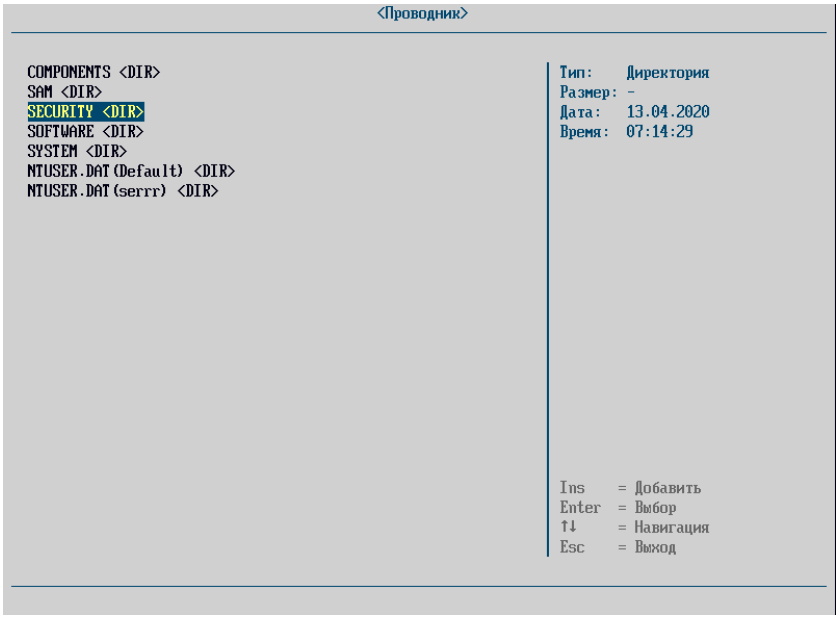

Рисунок 95 – Окно файлового браузера с разделами реестра

Контроль целостности возможен для следующих системных разделов реестра Windows:

– COMPONENTS (расположение \Windows\System32\config\COMPONENTS);

- SAM (расположение \Windows\System32\config\SAM);
- SECURITY (расположение \Windows\System32\config\SECURITY);
- SOFTWARE (расположение \Windows\System32\config\SOFTWARE);
- SYSTEM (расположение \Windows\System32\config\SYSTEM);
- DEFAULT (расположение \Windows\System32\config\DEFAULT);

Дополнительно в список контролируемых объектов могут быть добавлены пользовательские разделы реестра Windows (NTUSER.DAT). Данные разделы находятся в каталогах пользователей ОС Windows (каталог \Users\Test\ для пользователя с именем Test).

Так как файлов NTUSER.DAT может быть несколько, то к имени раздела добавляется в скобках имя пользователя для создания уникального имени раздела.

Внимание! Не рекомендуется добавлять в список контроля целостности корневые разделы (COMPONENTS, SOFTWARE, SYSTEM и т.д.) целиком, так как число файлов в разделе может достигать сотен тысяч. При этом добавление корневого раздела нецелесообразно, так как в процессе работы ОС Windows в раздел с большой вероятностью будут записаны данные, что приведет к нарушению целостности.

Внимание! Максимальное число отображаемых элементов в файловом браузере ограничено 2000. При входе в каталог, содержащий большее число дочерних элементов будет показано предупреждение, представленное на рисунке 96.

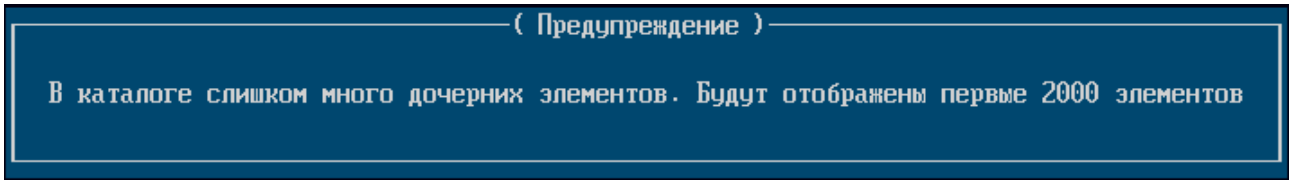

Рисунок 96 – Сообщение, отображаемое при большом числе дочерних элементов раздела реестра Windows

В случае если необходимо добавить неотображаемые элементы каталога, следует воспользоваться функцией импорта списка контроля целостности (см. раздел 5.7.4.1.4).

После выбора элемента реестра выполняется вычисление контрольной суммы элемента, а затем добавление элемента в список контроля целостности. При этом происходит возврат из файлового браузера в меню редактирования списка контроля целостности.

5.7.4.1.3. Редактирование списка контролируемых элементов

Нажатие клавиши «Delete» приводит к удалению выбранного элемента из списка контроля целостности.

Выбор пункта «Очистить список файлов» полностью очищает список контроля целостности.

Выбора пункта «Обновить контрольную сумму» пересчитывает контрольную сумму для каждого элемента из списка контроля целостности.

Выбор пункта «Сохранить список файлов» выполняет сохранение списка контроля целостности в NVRAM.

Максимальное число элементов, которые могут быть добавлены в список контроля

целостности: 1024.

5.7.4.1.4. Импорт/экспорт списка контроля целостности элементов реестра Windows

Импорт/экспорт списка контроля целостности осуществляется из главного окна управления контролем целостности реестра Windows.

Для экспорта настроек необходимо подключить USB-накопитель, на который будет осуществляется экспорт, перейти в меню «Контроль реестра Windows» выбрать пункт «Сохранить на USB». Список контроля целостности экспортируется в формате JSON в виде:

```
{
  "RegControlObjects": [
    {
      "DevPath": "VenHw(5CF32E0B-8EDF-2E44-9CDA-
93205E99EC1C,00000000)/VenHw(6888A4AE-AFCE-E84B-9102-
F7B9DAE6A030,00000000)/HKEY_LOCAL_MACHINE/",
      "File": "SYSTEM\\CurrentControlSet",
      "HashType": 5,
      "Hash":
"DACC4A629C0E39F186DA19C9A77D1A5548B147E99C432CC36921A3E846616C9F"
    },
    {
      "DevPath": "VenHw(5CF32E0B-8EDF-2E44-9CDA-
93205E99EC1C,00000000)/VenHw(6888A4AE-AFCE-E84B-9102-
F7B9DAE6A030,00000000)/HKEY_LOCAL_MACHINE/",
      "File": "SOFTWARE\\Intel",
      "HashType": 5,
      "Hash":
"F0579F6AA21128777E1A863363D0E26E0B8DC01E9B5BE6156F454B5F9E512455"
    },
    {
      "DevPath": "VenHw(5CF32E0B-8EDF-2E44-9CDA-
93205E99EC1C,00000000)/VenHw(6888A4AE-AFCE-E84B-9102-
F7B9DAE6A030,00000000)/HKEY_LOCAL_MACHINE/",
      "File": "SYSTEM\\RNG",
      "HashType": 5,
      "Hash":
"F840B896DEED410D322C2DBCC75E03FF3C8D698E99B298D9940B9BA89BE28C42"
    }
  ]
}
```

где

- DevPath – путь до раздела, содержащего реестр,
- File – путь до контролируемого элемента внутри реестра,
- HashType – тип контрольной суммы,
- Hash – контрольная сумма (параметр 5 указывается на хеш по алгоритму ГОСТ Р 34.11-2012, 256 бит).

Для импорта необходимо подключить USB-накопитель с файлом расширения JSON, выбрать пункт «Загрузить с USB», в открывшемся проводнике выбрать файл. Во время импорта список контроля целостности формируется из входного файла JSON. При это происходит сохранение сформированного списка в NVRAM.

Файл для импорта может быть сформирован вне Изделия. При этом для каждого

элемента обязательным будет являться только поле File.

Если поле DevPath не указано, то будет выполняться проверка первого найденного реестра.

Если поле HashType не указано, то будет взят алгоритм по умолчанию (ГОСТ Р 34.11-2012, 256 бит). В целях безопасности HashType со значениями меньше 5 запрещены. Если указано некорректное значение, то будет использоваться алгоритм по умолчанию.

Если поле Hash не указано, то контрольная сумма будет вычислена в процессе построения списка контроля целостности.

Например, корректным будет являться следующий файл JSON:

```
{
  "RegControlObjects": [
    {
      "File": "SYSTEM\\CurrentControlSet"
    },
    {
      "File": "SOFTWARE\\Intel"
    },
    {
      "File": "SYSTEM\\RNG"
    }
  ]
}
```

5.7.4.1.5. Контроль целостности элементов реестра Windows при загрузке ОС

Контроль целостности элементов осуществляется при каждой загрузке ОС. Если целостность элементов реестра нарушена, то выдается сообщение об ошибке:

```
«Ошибка! Нарушена целостность реестра Windows!»
```

Загрузка ОС при этом прекращается, а в журнал аудита добавляется запись.

5.7.4.1.6. Сопоставление содержимого реестра в Windows и в NumaArce

Представление реестра, отображаемое в утилите «regedit.exe» формируется из множества файлов, расположенных на системном разделе ОС Windows.

Физические файлы, участвующие в контроле целостности, отображаются в реестре Windows по следующим правилам:

- раздел COMPONENTS недоступен для редактирования с помощью regedit;
- раздел SAM соответствует ветке реестра HKEY_LOCAL_MACHINE\SAM\;
- раздел SECURITY соответствует ветке реестра HKEY_LOCAL_MACHINE\SECURITY\;
- раздел SOFTWARE соответствует ветке реестра HKEY_LOCAL_MACHINE\SOFTWARE\;
- раздел SYSTEM соответствует ветке реестра HKEY_LOCAL_MACHINE\SYSTEM\. При формировании раздела SYSTEM создается каталог CurrentControlSet, который является ссылкой на один из каталогов \SYSTEM\ControlSet00x, где x - число, записанное в файле \SYSTEM\Select\Current;
- раздел DEFAULT соответствует ветке реестра HKEY_USERS\.DEFAULT;

5.7.4.2. Secure Boot

Параметр Secure Boot включает проверку загрузки только подписанных образов ОС (EFI-модулей), т.е. при включенном значении параметра при попытке загрузить неподписанный образ ОС на экран выводится сообщение. И процесс загрузки завершается.

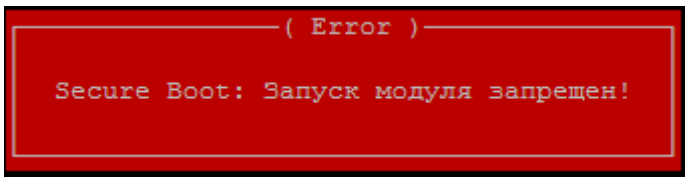

Рисунок 97 – Окно ошибки

5.7.4.3. Защита EFI-переменных

Параметр включает защиту EFI-переменных от изменений из ОС.

5.7.4.4. Контроль транзакций Ext4

Функция обеспечивает эмуляцию работы сервиса jbd2. При включенном параметре файловая система ext4 будет находиться в восстановленном состоянии.

Во время монтирования тома выполняется анализ журнала транзакций и сохранение всех блоков, которые необходимо восстановить. В дальнейшем при чтении файлов вместо того, чтобы читать блоки с диска, нужные блоки берутся из журнала транзакций, при чтении файла будет возвращено его конечное состояние, которое будет после загрузки ОС и работы сервиса jbd2. Если незавершенные транзакции каким-либо образом изменяют контролируемый файл, то процедура контроля целостности данного файла выполнится с ошибкой, и загрузка ОС будет остановлена.

Управление включением данного механизма анализа и эмуляции настраивается в меню «Параметры безопасности» → «Контроль транзакций Ext4». Для возможности использования данной функции в меню «Компоненты» необходимо включить «Linux-загрузку» для запуска драйвера ext.

5.7.4.5. Контроль целостности транзакций NTFS

Функция обеспечивает проверку файловой системы и настройку поведения Изделия при обнаружении незавершенных транзакций файловой системы NTFS. Изделие поддерживает следующие реакции:

– «Отключено» – проверка файловой системы не производится;

– «Предупреждение» – выводится предупреждающее сообщение;

– «Блокировка» – выводится предупреждающее сообщение, блокируется загрузка ОС. Дальнейшая загрузка доступна только после проверки администратором Изделия контрольных сумм.

5.7.4.6. Режим USB read-only

Данный параметр запрещает запись/экспорт информации на подключенный USB-накопитель до загрузки ОС. Экспорт информации (например, профилей загрузки, учетных карточек пользователей, сохранение файла-лицензии) или снимки экрана выполнены не будут. На экране будет отображаться ошибка сохранения/экспорта.

***Примечание**. Изменения вступят в силу только после перезагрузки СВТ.*

Наличие данной функции зависит от типа СВТ, на которое установлено Изделие.

5.7.5. «Проверка целостности»

Функция проверки целостности вручную предназначена для запуска принудительного контроля целостности бинарного образа Изделия, загружаемых компонент

операционной среды, журнала аудита, профилей пользователей.

Для запуска проверки необходимо выполнить следующие действия:

– авторизоваться под учётной записью административного пользователя (администратор, аудитор);

– выбрать пункт основного меню «Проверка целостности».

На экран будет выведено сообщение с результатами проверки всех компонентов (см. рисунок 98).

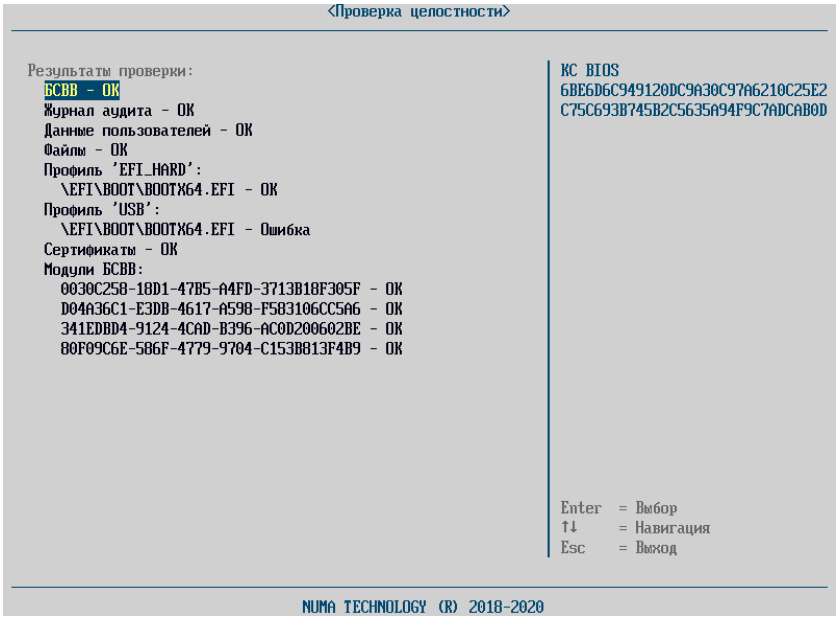

Рисунок 98 – Результат контроля целостности вручную

При наведении клавишами «↓» и «↑» в правой части окна синим шрифтом выводится хеш–сумма выделенной строки.

Управление списком файлов профиля загрузки, для которых осуществляется контроль целостности, доступно из раздела «Панель управления» → «Конфигуратор» → «Редактирование профиля».

***Примечание**. В случае нарушения целостности загружаемого профиля загрузки необходимо выполнить действия, описанные в Приложении 7.*

5.7.6. «Контроль оборудования»

Контроль оборудования проверяет добавление, удаление, замену аппаратных компонент. Перестановка однотипных устройств в местах подключения (слоты памяти, SATA-порты) также считается нарушением контроля.

Контроль оборудования может функционировать в следующих режимах:

– контроль отключен;

– полный контроль;

– базовый контроль;

– настраиваемый контроль.

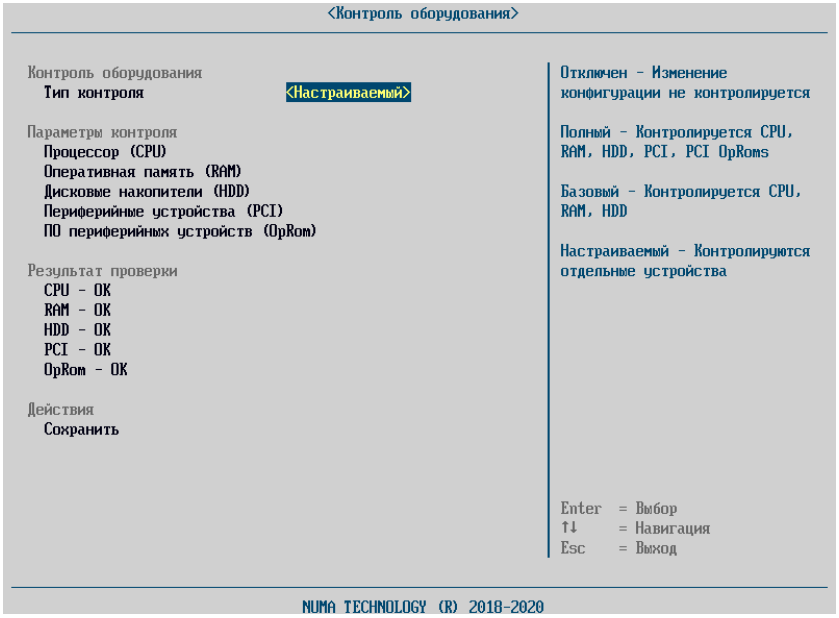

Рисунок 99 – Главное окно контроля оборудования

В режиме отключения контроля замена/добавление/удаление аппаратных компонентов не проверяется.

При полном контроле проверяется целостность CPU, RAM, HDD, PCI, PCI OpRoms, регион ME микросхемы SPI-flash-памяти.

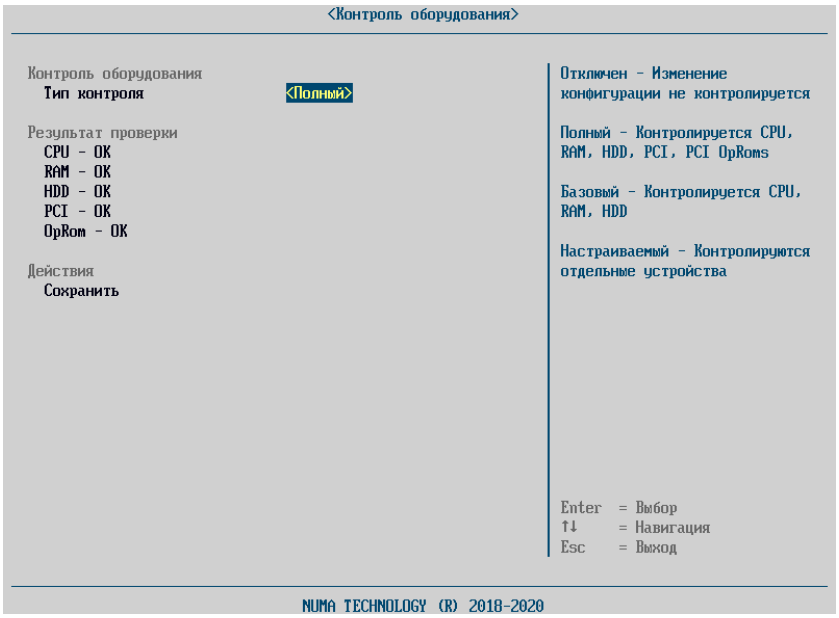

Рисунок 100 – Тип контроля оборудования «Полный»

В режиме базового контроля проверяется целостность CPU, RAM, HDD. Устройства PCI и OpRoms отключаются от контроля.

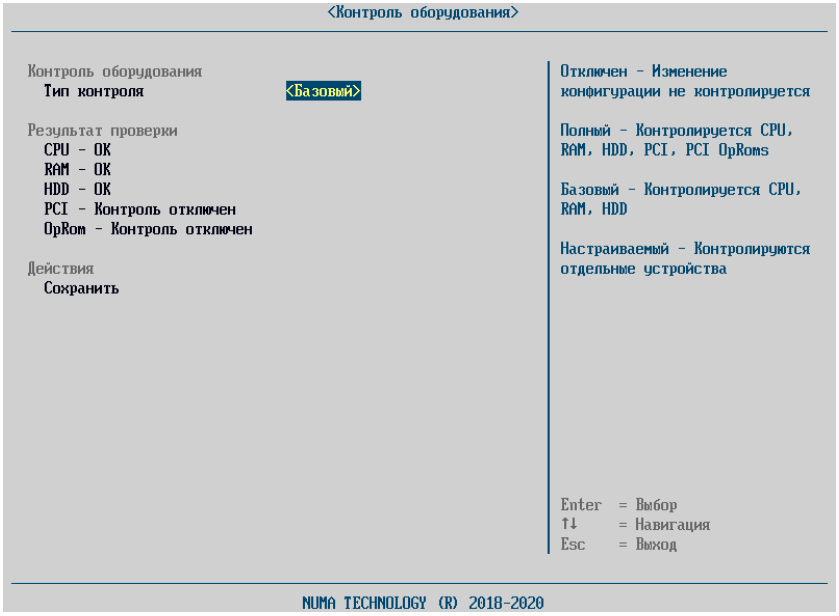

Рисунок 101–Тип контроля оборудования «Базовый»

Настраиваемый контроль позволяет гибко управлять контролем аппаратной платформы. Появляется возможность включения/выключения отдельных типов устройств и отдельных устройств из контроля. В режиме базового и полного контроля такие возможности отсутствуют.

На рисунке 102 представлено окно меню «Контроль оборудования» в режиме настраиваемого контроля.

Рисунок 102 – Тип контроля оборудования «Настраиваемый»

Добавление, удаление или перестановка контролируемых устройств приводит к нарушению контроля целостности. При нарушении контроля целостности невозможна загрузка ОС из профилей загрузки.

При попытке загрузки выдается сообщение об ошибке:

«Ошибка! Нарушена целостность оборудования!»

и загрузка ОС прекращается.

В режиме администрирования проверка целостности оборудования выполняется при каждом входе в меню контроля оборудования. Если КС аппаратной конфигурации не

совпадает с сохраненной, то выдается сообщение об ошибке (см. рисунок 103).

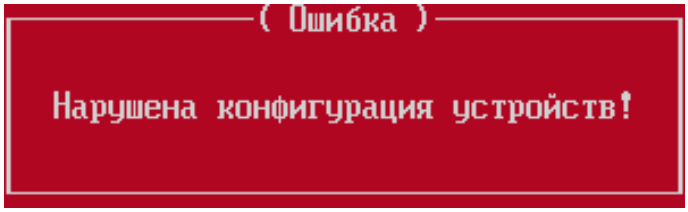

Рисунок 103 – Сообщение об ошибке контроля целостности аппаратной платформы

При переходе в меню «Контроль оборудования» можно посмотреть какой тип устройств привел к нарушению целостности. Например, при нарушении целостности устройства RAM (возможно, нарушение произошло из-за подключения или отключения устройства, или подключения заново устройства в другой порт) в меню «Контроль оборудования» напротив устройства RAM будет отображаться «Ошибка».

В данном режиме доступна настройка отдельных типов устройств. На рисунке 104 представлено окно настройки параметров устройств PCI.

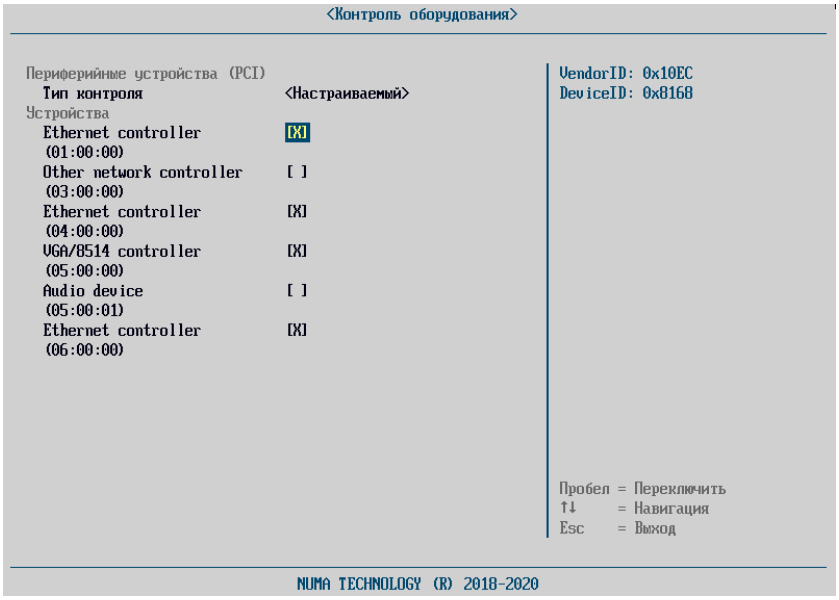

Рисунок 104 – Настройка параметров контроля устройств PCI

Для типов устройств доступны следующие типы контроля:

1) отключен – устройства данного типа не контролируются;
2) полный – контролируются все подключенные устройства данного типа;
3) настраиваемый – имеется возможность включения/выключения отдельных устройств из контроля целостности.

Настройка параметров контроля ПО периферийных устройств (OpRom) зависит от настройки параметров периферийных устройств (PCI). Контроль OpRom осуществляется по следующим правилам:

1) если выключен контроль устройств PCI, то устройства OpRom также не контролируются. При этом пункт настройки контроля OpRom недоступен для выбора;
2) если из контроля выключены отдельные устройства PCI, то их OpRom также не проверяется;
3) если устройство PCI проверяется, то при этом можно выключить контроль его OpRom. Для этого необходимо выбрать в пункте настройки OpRom настраиваемый режим и исключить целевое устройство из контроля.

В процессе контроля PCI также проверяются устройства на нулевой шине (устройства PCH). При этом администратору доступны для настройки только внешние устройства PCI (PCI-шина 1 и выше). При проверке целостности PCI игнорируется локация устройства (BUS, DEV, FUNC), так как список шин при подключении/отключении периферийных устройств формируется динамически. Это приводит к ситуации, когда при подключении внешнего устройства меняются BUS уже подключенных ранее устройств. Это делает невозможным реализацию выключения отдельных устройств из контроля целостности PCI. По этой же причине не проверяются устройства типа PCI BRIDGE, так как данные устройства включаются/отключаются динамически (в том числе на нулевой шине) при подключении внешних устройств PCI. Таким образом, в процессе контроля PCI неявно проверяются PCI-устройства Intel, расположенные на нулевой шине. Администратор может выключать из контроля только PCI-устройства, расположенные выше нулевой шины. При подключении/отключении внешних PCI-устройств может меняться BUS, DEV для уже подключенных устройств. Поэтому полная локация устройства носит справочный характер, а фактически устройства сравниваются по Vendor ID, Device ID ClassCode – данные отображаются в области справки при выборе PCI-устройства в контроле оборудования.

После завершения ввода параметров администратору необходимо сохранить изменения, выбрав пункт «Сохранить» на главной странице контроля оборудования. При этом будет выполнена запись параметров в NVRAM SPI-flash.

При сохранении контрольная сумма конфигурации пересчитывается и записывается в NVRAM. При каждом входе в настройки контроля оборудования и при каждом загрузке ОС из конфигурации вычисляется текущая КС аппаратной конфигурации и сравнивается с расположенной в NVRAM.

5.7.7. Дополнительные параметры

5.7.7.1. Проверка отзыва сертификата

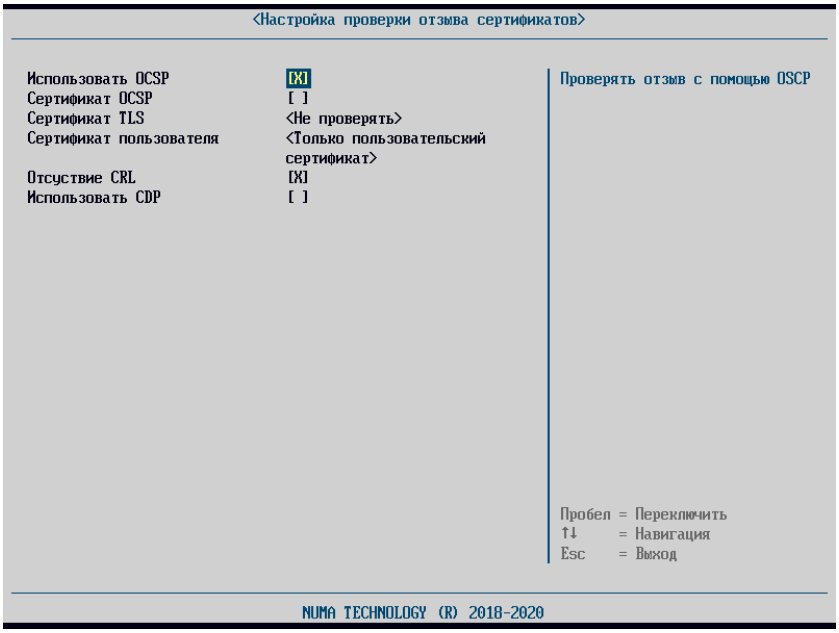

Рисунок 105 – Меню «Настройка проверки отзыва сертификатов»

Для настройки проверки отзыва сертификатов доступны следующие настраиваемые параметры:

«Использовать OCSP» – пункт меню отвечает за использование протокола OCSP (Online Certificate Status Protocol) во время процедуры верификации сертификатов. URI OCSP сервера берется из проверяемых сертификатов. OCSP запрос выполняется как при проверке пользователя (сертификата в токене), так и при создании TLS соединения, при проверке

сертификата сервера;

«Сертификат OCSP» – контролирует возможность проверки отзыва сертификата подписи OCSP с помощью CLR;

«Сертификат TLS» – данное поле отвечает за проверку отзыва сертификатов с помощью CRL при установке защищенного TLS соединения к LDAP. В случае если CRL будет отсутствовать и не будет выполнен OCSP запрос, то TLS соединение не установится. Доступно три значения параметра «Не проверять», «Всю цепочку», «Только сертификат сервера».

«Проверка пользовательского сертификата» – проверка отзыва сертификата пользователя с помощью CRL;

«Использовать CDP» – отвечает за использование CDP в качестве источника CRL. При выставленном флаге в данном поле необходимо либо ввести «CDP URL», либо выставить поле «Читать CDP сертификата».

5.8. Раздел «Информация»

5.8.1. Меню «Ключ OA 3.0»

Данный пункт предназначен для выполнения OEM (OA3.0) активации Windows. Форма «Windows OEM Activation» содержит поле для ввода цифрового ключа продукта (DPK) в формате: «XXXXX-XXXXX-XXXXX-XXXXX-XXXXX». Администратор вводит значение ключа и нажимает кнопку «Сохранить». После этого дальнейшая корректировка невозможна!

Цифровой ключ продукта прошивается в BIOS компьютера. Windows активируется автоматически при первом подключении компьютера к интернету.

OEM-версия предназначена для поставок только с новым оборудованием и непригодна для обновления уже существующей операционной системы, поддерживает только чистую новую установку. Эта версия требует активации в течение тридцати суток с момента установки.

5.8.2. Меню «Монитор состояний»

Данное меню позволяет отслеживать состояние и скорость оборотов датчиков вентилятора, а также определять значение температуры системы (System), температуру центрального процессора (CPU).

Примечание. *Датчики могут быть изменены в зависимости от типа СВТ, на которое установлено Изделие.*

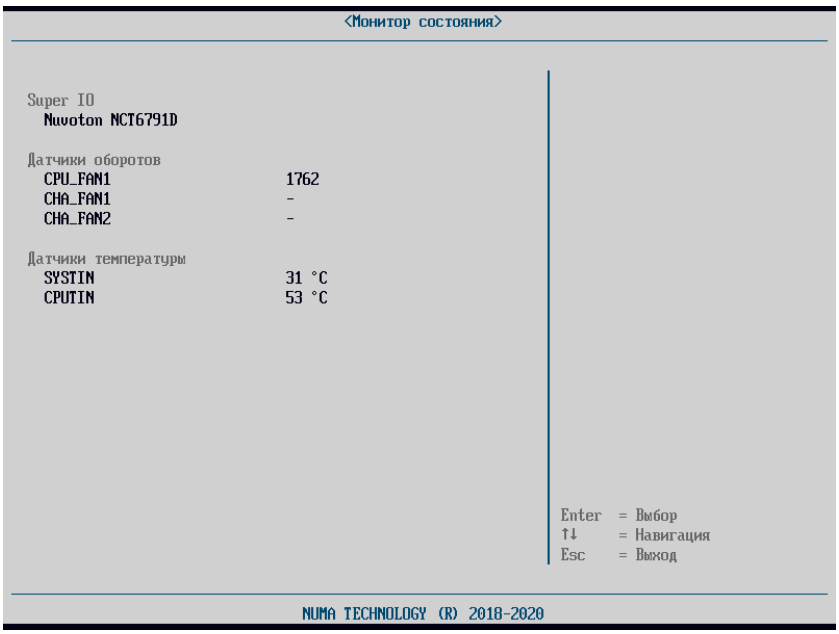

Рисунок 106 – Форма меню «Монитор состояний»

5.8.3. «Системная информация»

Выбрав пункт меню «Системная информация», можно получить сведения о параметрах процессора, оперативной памяти, устройствах в SATA-портах, адресах сетевых контроллеров, используемых в системе аппаратных ресурсов (см. рисунок 107).

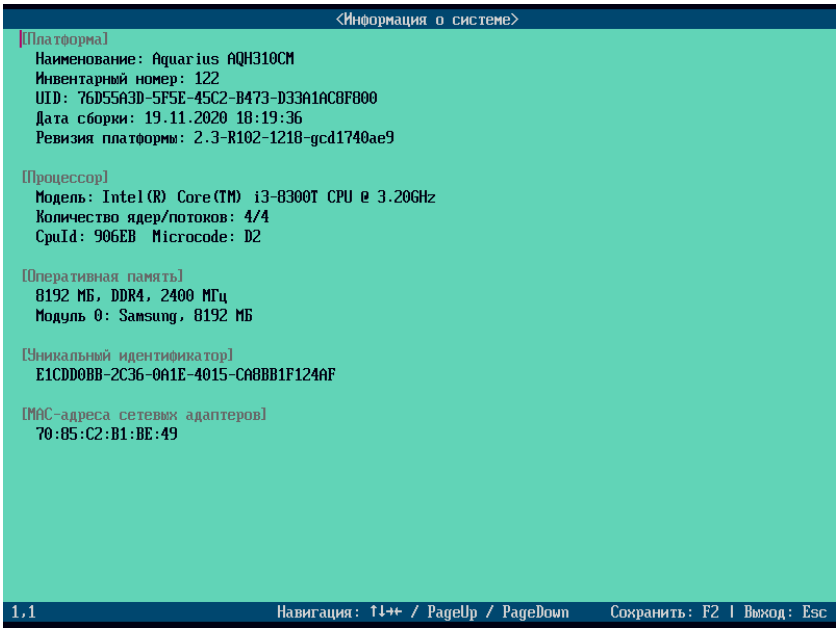

Рисунок 107 – Информация о системе

5.8.4. «Версия БСВВ»

Пункт меню «Версия БСВВ» показывает текущую версию прошивки Изделия, информацию о лицензии и позволяет обновить версию Изделия (см. рисунок 108).

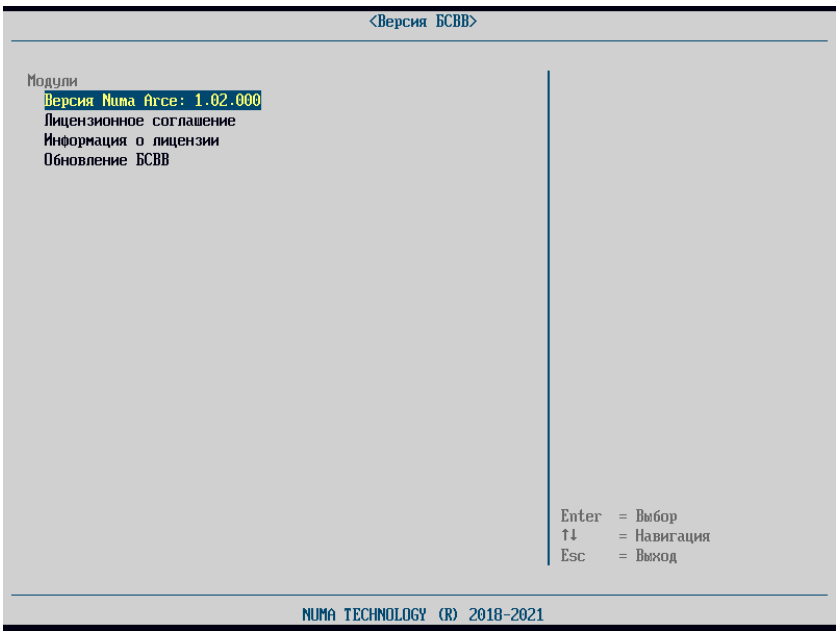

Рисунок 108 – Раздел версия Изделия

В первом пункте с версией Изделия указывается основная информация разработчика об Изделии. Пример отображения версии Изделия представлен на рисунке 109.

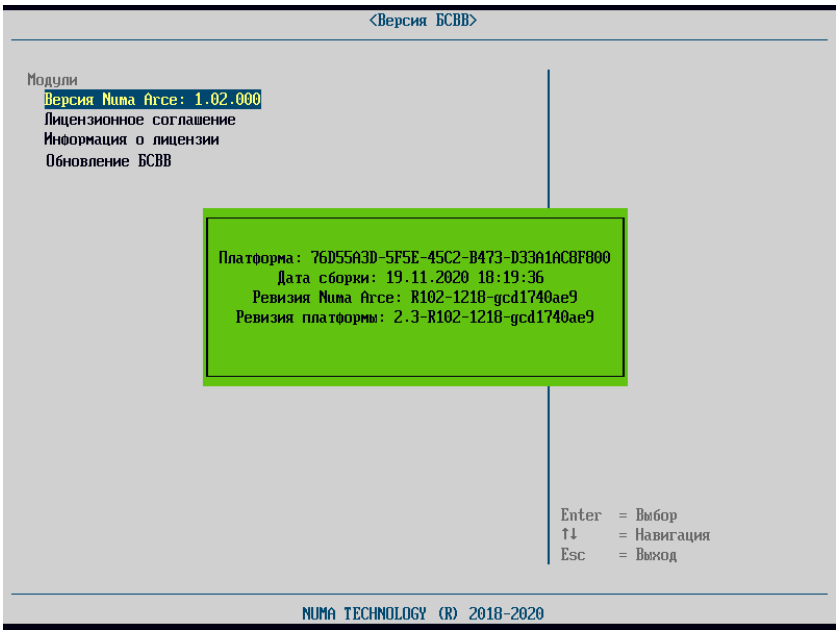

Рисунок 109 – Версия Изделия

5.8.4.1. Лицензионное соглашение

При выборе этого пункта на экран выводится текст лицензионного соглашения. Пролистывание текста доступно как построчно, с помощью клавиш «↓» «↑», так и постранично, с использованием клавиш «PgUp/PgDown».

5.8.4.2. Информация о лицензии

Форма имеет вид, представленный на рисунке 110 и предназначена для:

– отображения текущего состояния лицензии;

– управления лицензией.

Раздел [Информация] отображает поля:

– «Тип лицензии» с допустимыми значениями – Обычная (бессрочная) или Пробная (ограниченный срок действия);

– «Функция» допустимые значения – БСВВ или МДЗ.

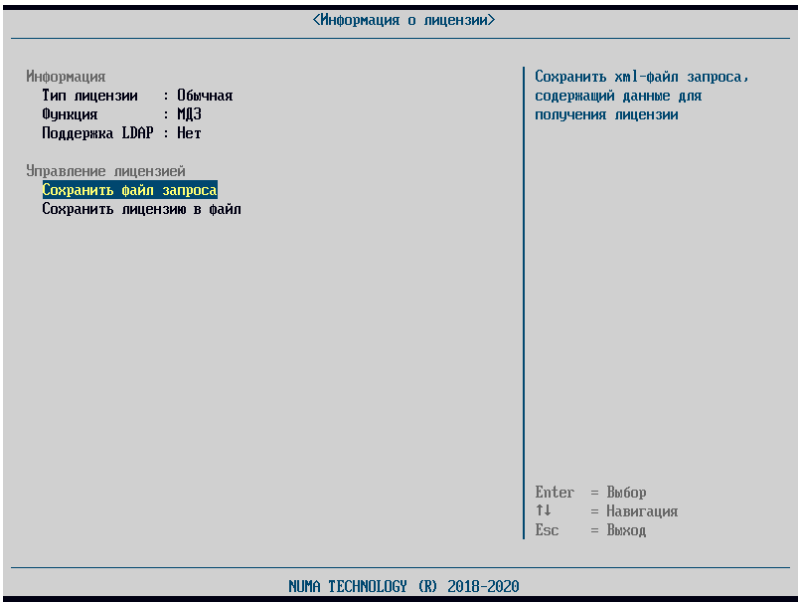

Рисунок 110 – Меню информация о лицензии

В разделе «Управление лицензией» можно выполнить формирование запроса на лицензию, например, при замене пробной лицензии на постоянную.

О необходимости такой замены, Изделие информирует сообщением:

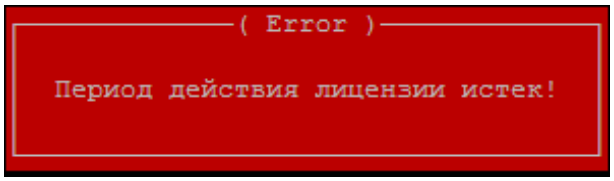

Рисунок 111 – Окно ошибки истекшей лицензии

Для формирования файла-запроса необходимо:

– подключить USB-накопитель в СВТ;

– «Сохранить файл запроса». Необходимые данные будут сохранены на USB-накопитель в файл с именем «numa_license_req_XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX.xml».

Созданный файл необходимо отправить в сервисную службу ООО «НумаТех» по электронной почте, указанной в документе «Формуляр» 643.АМБН.00002-01 30 01.

На основе файла запроса лицензии будет создан файл лицензии («XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX.p12»).

Для активации лицензии необходимо полученный файл лицензии загрузить через пункт меню «Загрузить файл лицензии». После проверки лицензии работа Изделия будет разблокирована (см. рисунок 112), Изделие будет доступно для дальнейшей настройки и использования.

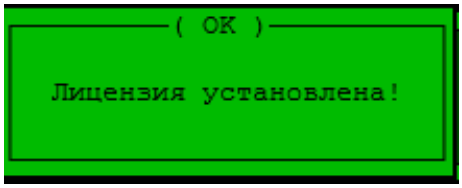

Рисунок 112 – Успешная установка лицензии

В случае если выбран файл от неверной платформы, появляется сообщение об ошибке – «Проверка лицензии завершилась с ошибкой!». В этом случае необходимо проверить соответствие устанавливаемого файла с техническими характеристиками устройства, на которое производится установка. При появлении ошибки повторно следует обратиться в службу технической поддержки Изготовителя СВТ, на которое устанавливается Изделие, или в сервисную службу компании ООО «НумаТех» по электронной почте, указанной в документ «Формуляр» 643.АМБН.00002-01 30 01.

5.8.4.3. Обновление БСВВ

Внимание! Не допускается выключение питания во время обновления.

***Примечание**. Для установки/обновления Изделия требуется USB-накопитель с файловой системой FAT32.*

Внимание! Процедура безопасной установки/обновления Изделия должна начинаться с проверки контрольной суммы полученного Изделия на соответствие сертифицированной версии! Процедура выполняется согласно документу «Инструкция по проверке контрольных сумм» 643.АМБН.00002-01 94 01.

Для обновления необходимо выполнить следующие действия:

1) выгрузить журнал аудита согласно разделу 5.7.3. Изделие не позволит начать обновление до выгрузки всего журнала аудита на USB-носитель;
2) проверить контрольную сумму полученного от производителя ПО (или Изготовителя устройства) файла-прошивки согласно прилагаемой к файлу инструкции;
3) записать файл-прошивку на USB-накопитель и подключить к СВТ;
4) включить СВТ;
5) в меню «Панель управления» выбрать пункт «Версия БСВВ» → «Обновление БСВВ»;
6) в открывшемся списке файлов выбрать файл-прошивку и нажать «Enter»;
7) в появившемся окне подтвердить проведение обновления;

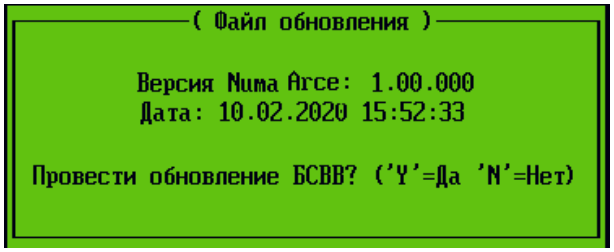

Рисунок 113 – Диалоговое окно обновления

8) в появившемся окне «Обновить EFI-переменные?», нажать «Y»;
9) подтвердить действия нажатием «Enter» в следующем окне;
10) начнется запись образа прошивки в флеш-память.

По окончании обновления будет показано сообщение (см. рисунок 114) и СВТ будет выключен.

Рисунок 114 – Сообщение об успешном обновлении Изделия

При выборе несоответствующего данной аппаратной платформе бинарного файла обновления Изделие выдаст сообщение об ошибке (см. рисунок 115).

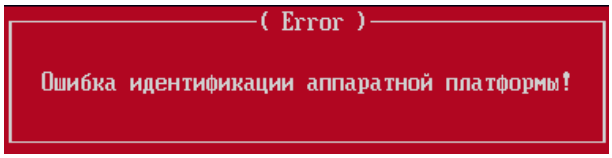

Рисунок 115 – Сообщение о некорректном файле обновления Изделия

6. СООБЩЕНИЯ АДМИНИСТРАТОРУ

6.1. Режим начальной инициализации

Сообщения, которые могут появиться при подготовке к работе Изделия, приведены в таблице ниже.

Таблица 1 – Сообщения в режиме подготовке к работе Изделия

Сообщение	Описание	Действие
«Нарушена целостность БСВВ»	Произошло вмешательство извне в бинарный образ БСВВ	Уведомить администратора и ответственного за безопасность информации
«Введите начальный пароль»	Режим подготовки к работе	Ввести логин и пароль
«Пароль не верен»	Режим подготовки к работе	Повторно ввести пароль
«Создание карточки администратора»	Режим подготовки к работе	Задать карточку администратора
«Ошибка создания карточки администратора: не хватает данных»	При создании карточки администратора не были введены обязательные поля	Задать все поля данных
«Ошибка создания карточки администратора: данные сопоставления не верны»	Ошибка при задании данных сопоставления АНП	Задать верные данные
«Восстановление настроек с внешнего носителя»	Функция восстановления настроек	
«Ошибка восстановления: нет носителя»	Нет USB Flash-диска	Вставить USB Flash-диск в USB-порт
«Ошибка восстановления: неподдерживаемый носитель»	USB Flash–диск имеет неподдерживаемую файловую систему	Предъявить диск с поддерживаемой файловой системой
«Ошибка восстановления»	При восстановлении настроек произошла ошибка	Повторить заново, либо обратиться в сервисный центр

6.2. Режим администрирования

Сообщения БСВВ, которые могут появиться в режиме администрирования, приведены в таблицах ниже.

Таблица 2 – Сообщения при восстановлении настроек с внешнего носителя

Сообщение	Описание	Действие
«Ошибка восстановления: нет носителя»	Нет USB Flash–диска	Вставить USB Flash–диск в USB–порт

Сообщение	Описание	Действие
«Ошибка восстановления: неподдерживаемый носитель»	USB Flash–диск имеет неподдерживаемую файловую систему	Предъявить диск с поддерживаемой файловой системой
«Ошибка восстановления»	При восстановлении настроек произошла ошибка	Повторить заново либо обратиться в сервисный центр
Введите PIN код	Авторизация на АНП	Ввести PIN–код
«PIN код не верен»	Предъявлен неверный PIN код	Предъявить верный PIN–код
«Ошибка выгрузки: нет носителя»	Нет USB Flash–диска	Вставить USB Flash–диск USB–порт
«Ошибка выгрузки: неподдерживаемый носитель»	USB Flash–диск имеет неподдерживаемую файловую систему	Предъявить диск с поддерживаемой файловой системой
«Данные инсталляционного носителя не верны»	Носитель не является доверенным и содержащим ПО	Обратиться к администратору безопасности
«Ошибка контроля целостности инсталляционного носителя»	Носитель не является доверенным и содержащим ПО	Обратиться к администратору безопасности

Таблица 3 – Сообщения при загрузке/обновлении сертификатов УЦ

Сообщение	Описание	Действие
«Ошибка! Неизвестный формат PKCS7 цепочки CA!»	Файл не является файлом цепочки сертификатов, или формат цепочки не DER	Выбрать файл формата DER
«Ошибка! Неизвестный формат CRL»	Файл не является файлом цепочки сертификатов, или формат цепочки не DER	Выбрать файл цепочки сертификатов формата DER
«Сертификат еще не вступил в действие»	Срок действия загружаемого сертификата еще не наступил.	Выбрать сертификат с корректным сроком действия

6.3. Штатный режим

Сообщения БСВВ, которые могут появиться в штатном режиме, приведены в таблице ниже.

Таблица 4 – Сообщения в штатном режиме

Сообщение	Описание	Действие
«Нарушена целостность БСВВ»	Произошло вмешательство извне в бинарный образ БСВВ	Срочно уведомить администратора комплекса и ответственного за безопасность
«Введите PIN код»	Авторизация на АНП	Ввести PIN–код
«PIN код не верен»	Предъявлен неверный PIN–код	Предъявить верный PIN–код

ПРИЛОЖЕНИЕ 1

ДАННЫЕ СОПОСТАВЛЕНИЯ

Данные сопоставления задаются в текстовом файле в следующем виде:

```
тип данных сопоставления1=значение данных
тип данных сопоставления2=значение данных
```

Пример задания данных сопоставления:

```
CN=cn token user1
SUBJECT=subject for token user1
MAIL=token_user1@NUMA.ru
UID=1234
DIGEST=11223344556677889900112233445566778899001122334455667788990011
22
```

Ограничения:

– обрабатывается не более 5 строк;

– при дублировании типов будет использован первый по порядку следования в файле.

ПРИЛОЖЕНИЕ 2

ПОРЯДОК СЛЕДОВАНИЯ ПОЛЕЙ ПРИ СОЗДАНИИ КАРТОЧЕК ПОЛЬЗОВАТЕЛЕЙ

Карточки пользователей задаются в Unicode JSON-файле.

Порядок следования полей в общем случае указан в таблице 5, для пользователей «логин/пароль» – в примере 1, для пользователей «АНП» – в примере 2, для пользователей «АНП+логин/пароль» – в примере 3.

Таблица 5 – Порядок следования полей

Поле	**Значение**	**Описание**
Name	UNICODE, от 3 до 25 символов	Логин
UserID	Число	Идентификатор пользователя
AuthType	«Password», «Token», «TokenAndPassword»	Тип аутентификации: Password – логин/пароль, Token – АНП, TokenAndPassword – АНП + логин/пароль
Flags	Число	Битовые флаги, объединенные по "или": 128 – для административных пользователей; 0 – для пользователей.
FullName	UNICODE, не более 25 символов	ФИО пользователя
ContactInfo	UNICODE, не более 50 символов	Контактная информация
TokenData	Массив полей	Поля данных сопоставления
Type	«SN», «Digest», «Mail»	Тип сопоставления: SN – Subject name, Digest - хеш, Mail – эл.почта
ComparisonData	Текстовое значение	Данные сопоставления
AccessType	0/2/4	Роль пользователя. Возможные значения: 4 – Пользователь, 2 - Администратор, 0 - Аудитор
PasswordCreationTime	Дата и время в UNICODE	Время создания пароля
PasswordHash	строка	Хеш-значение пароля

Пример 1 – Пример для пользователя типа «логин/пароль»:

```
{
      "Name": "admin",
      "UserID": 1,
      "AuthType": "Password",
      "Flags": 128,
      "FullName": "admin",
      "ContactInfo": "admin",
      "PasswordCreationTime": "2021-07-09_16:52:22",
      "PasswordHash":
"CCE01BC759820155312E16243835DC2124900C00B9D4CC8671B07100F0A34C33",
      "AccessType": 3
    }
```

Пример 2 – Пример для пользователя типа «АНП»:

```
{
      "Name": "ANP",
      "UserID": 2,
      "AuthType": "Token",
      "Flags": 128,
      "FullName": "Asd",
      "ContactInfo": "Asd",
      "TokenData": [
        {
          "Type": "CN",
          "ComparisonData": "NEO2"
        }
      ],
      "AccessType": 2
    }
```

Пример 3 – Пример для пользователя типа «АНП+логин/пароль»:

```
{
  "UsersList": [
    {
      "Name": "qwe",
      "UserID": 3,
      "AuthType": "TokenAndPassword",
      "Flags": 128,
      "FullName": "qweqweqwe",
      "ContactInfo": "qwe",
      "TokenData": [
        {
          "Type": "SN",
          "ComparisonData": "000000003E2E5A51"
        },
        {
          "Type": "DIGEST",
          "ComparisonData":
"5F38037EA9274D242F303749473ED5016A4365C6391A31FF836FD9420AB36C19"
        }
      ],
      "PasswordCreationTime": "2021-10-24_19:16:31",
      "PasswordHash":
"71479DC11EB2C1FDAFE1A433B2ACCBC0A70247266B538C48EC9E2CB4188C299C",
      "AccessType": 2
    }
  ]
}
```

ПРИЛОЖЕНИЕ 3

СПИСОК СОБЫТИЙ, РЕГИСТРИРУЕМЫХ В ЖУРНАЛЕ

Код события	Мнемоника	Уровень критичности		Описание
0x0002	HEVENT_USER_LOGIN	6/3	Информация (info) Ошибка (error)	Авторизация пользователя, событие заносится в журнал при каждой попытке авторизации с результатом «успех» или «ошибка» в зависимости от результата прохождения авторизации
0x0003	HEVENT_ADD_NEW_USER	6/3	Информация (info) Ошибка (error)	Создание (добавление) нового пользователя, заносится в журнал при каждой записи во флеш новой карточки пользователя
0x0004	HEVENT_DELETE_USER	6/3	Информация (info) Ошибка (error)	Удаление пользователя из системы БСВВ, заносится в журнал при удалении карточки пользователя
0x0005	HEVENT_LOAD_CA	6	Информация (info)	Загрузка сертификата удостоверяющего центра, заносится при записи во флеш данных сертификата
0x0006	HEVENT_LOAD_CRL	6	Информация (info)	Загрузка списка отозванных сертификатов, заносится при записи во флеш данных сертификата
0x0009	HEVENT_FORCE_CHECK_INTEGRITY	6/3	Информация (info) Ошибка (error)	Принудительный контроль целостности, заносится в журнал при выполнении контроля целостности из меню
0x000A	HEVENT_START_TO_LOAD_OS	6/3	Информация (info) Ошибка (error)	Старт запуска ОС, событие заносится в журнал перед каждой загрузкой ОС с результатом «успех» и в случае если загрузка ОС не прошла, т. е. вернулись из загрузчика в БСВВ с результатом «Ошибка»
0x000C	HEVENT_ADMIN_MODE	7	Отладочная (debug)	Вход в меню режима администрирования, заносится при входе в меню «Панель управления»

Код события	Мнемоника	Уровень критичности		Описание
0x000D	HEVENT_USER_UPDATE_DATA	6/3	Информация (info) Ошибка (error)	Обновление данных учетной записи пользователя
0x000E	HEVENT_CHECK_MODULE	3	Ошибка (error)	Проверка целостности модуля перед загрузкой ОС, заносится при проверке списка контроля целостности для выбранного способа загрузки (например, «Загрузка профиля» в Главном меню)
0x000F	HEVENT_EXPORT_USERS	6/3	Информация (info) Ошибка (error)	Экспорт учетных записей пользователей на USB накопитель
0x0010	HEVENT_ADMIN_MODE_EXIT	7	Отладочная (debug)	Выход из меню "Панель управления", заносится в журнал при выборе профиля загрузки
0x0011	HEVENT_CERT_MODE_ENTER	7	Отладочная (debug)	Вход в меню управления сертификатами
0x0012	HEVENT_CERT_MODE_EXIT	7	Отладочная (debug)	Выход из меню управления сертификатами
0x0013	HEVENT_USR_CTRL_MODE_ENTER	7	Отладочная (debug)	Вход в меню управления пользователями
0x0014	HEVENT_USR_CTRL_MODE_EXIT	7	Отладочная (debug)	Выход из меню управления пользователями
0x0015	HEVENT_DATE_TIME_MODE_ENTER	7	Отладочная (debug)	Вход в меню дата/время
0x0016	HEVENT_DATE_TIME_MODE_EXIT	7	Отладочная (debug)	Выход из меню дата/время

Код события	Мнемоника	Уровень критичности		Описание
0x0017	HEVENT_RESET_SYSTEM	7	Отладочная (debug)	Перезагрузка системы
0x0019	HEVENT_ADM_MODE_EXIT	5	Уведомление (notice)	Завершение режима администрирования, заносится в журнал при нажатии ESC в меню "Панель управления" с дальнейшей перезагрузкой
0x001A	HEVENT_TOKEN_EJECTED	5	Уведомление (notice)	Уведомление об извлечении токена
0x001B	HEVENT_BIOS_UPDATE_MODE_ENTER	7	Отладочная (debug)	Вход в пункт меню «ВерсияБСВВ\обновления БСВВ»
0x001C	HEVENT_BIOS_UPDATE_MODE_EXIT	7	Отладочная (debug)	Выход в пункт меню «ВерсияБСВВ\обновления БСВВ»
0x001F	HEVENT_HISTORY_MENU_ENTER	7	Отладочная (debug)	Вход в меню «Управления журналом аудита»
0x0020	HEVENT_HISTORY_MENU_EXIT	7	Отладочная (debug)	Выход из меню «Управления журналом аудита»
0x0021	HEVENT_USR_PASS_CHANGE	6	Информация (info)	Смена пароля пользователя
0x0022	HEVENT_TOKEN_INSERT_NOTIFY	5	Уведомление (notice)	Подключен токен
0x0023	HEVENT_USER_NAME_FAIL	3	Ошибка (error)	Неверное имя пользователя, заносится в журнал при вводе неверного имени пользователя

Код события	Мнемоника	Уровень критичности		Описание
0x0024	HEVENT_WRONG_PIN	3	Ошибка (error)	Введен неверный PIN -код, заносится в журнал при вводе неверного PIN-кода, при авторизации по токену
0x0026	HEVENT_DEV_MANAGER_MODE_ENTER	7	Отладочная (debug)	Вход в меню «Драйверы устройств»
0x0027	HEVENT_DEV_MANAGER_MODE_EXIT	7	Отладочная (debug)	Выход из меню «Драйверы устройств»
0x003E	HEVENT_MAX_WRONG_PIN_REACHED	2	Критическая ошибка (critical)	Достигнуто максимальное количество подряд неверно введённых ПИН-кодов для токена
0x003F	HEVENT_UNKNOWN_FORMAT_OF_CRL	3	Ошибка (error)	Неизвестный формат CRL
0x0040	HEVENT_UNKNOWN_FORMAT_OF_CERT	3	Ошибка (error)	Неизвестный формат сертификата
0x0041	HEVENT_UNKNOWN_KEY_FORMAT	3	Ошибка (error)	Неизвестный формат ключа
0x0042	HEVENT_ERR_CA_SIGN	3	Ошибка (error)	Ошибка при проверке подписи CA
0x0043	HEVENT_ERR_CERT_REVOKED	3	Ошибка (error)	Сертификат отозван
0x0044	HEVENT_ERR_GET_CA_PUBKEY	3	Ошибка (error)	Ошибка при извлечении открытого ключа CA
0x0045	HEVENT_ERR_CRL_VERIFY	3	Ошибка (error)	Ошибка при проверке подписи CRL

Код события	Мнемоника	Уровень критичности		Описание
0x0047	HEVENT_VERIFY_ERROR	3	Ошибка (error)	Ошибка верификации структуры данных
0x0048	HEVENT_ERROR_TO_LOAD_CRL	3	Ошибка (error)	CRL не загружен
0x0049	HEVENT_ERROR_TO_LOAD_ISSUER_CERT	3	Ошибка (error)	Цепочка CA не полная. Не найден сертификат Issuer
0x004A	HEVENT_ERROR_TO_LOAD_ISSUER_CERT_LOCALLY	3	Ошибка (error)	Отсутствует сертификат CA, подписавший сертификат пользователя
0x004C	HEVENT_CERT_NOT_YET_VALID	3	Ошибка (error)	Сертификат еще не вступил в действие
0x004D	HEVENT_CERT_HAS_EXPIRED	3	Ошибка (error)	Срок действия сертификата истек
0x004E	HEVENT_CRL_HAS_EXPIRED	3	Ошибка (error)	Срок действия CRL истек
0x004F	HEVENT_UNABLE_TO_GET_CRL	3	Ошибка (error)	Не найден CRL для проверки сертификата/цепочки CA
0x0050	HEVENT_BOOT_CFG_CHANGE	6/3	Информация (info) Ошибка (error)	Изменение профиля загрузки
0x0051	HEVENT_BOOT_ICFL_CHANGE	6/3	Информация (info) Ошибка (error)	Изменение списка контроля целостности для профиля загрузки
0x0052	HEVENT_PRIMARY_VIDEO_CHANGE	6/3	Информация (info) Ошибка (error)	Изменение конфигурации чипсета: изменен первичный видеоадаптер

Код события	Мнемоника	Уровень критичности		Описание
0x005B	HEVENT_HISTORY_SEVERITY_LVL_CHANGE	1	Тревога (alert)	Изменение уровня записи в журнал
0x005C	HEVENT_HISTORY_AUTO_CLR_CHANGE	6	Информация (info)	Изменение параметра «автоматическая очистка» в меню «Управления журналом аудита»
0x005D	HEVENT_QUICK_BOOT_START	6	Информация (info)	Выполнение загрузки из меню «Быстрая загрузка»
0x005E	HEVENT_QUICK_BOOT_END	6/3	Информация (info) Ошибка (error)	Результат выполнения (завершения) загрузки из меню «Быстрая загрузка»
0x005F	HEVENT_REGULAR_BOOT	6	Информация (info)	Загрузка профиля загрузки
0x0060	HEVENT_ADMIN_BOOT	6	Информация (info)	Выбор пункта меню "Панель управления"
0x0063	HEVENT_BOOT_MNGR_IMPORT_OPT	6	Информация (info)	Импорт профилей загрузки с USB накопителя
0x0064	HEVENT_BOOT_MNGR_EXPORT_OPT	6	Информация (info)	Импорт профилей загрузки на USB накопитель
0x0065	HEVENT_REVOKE_CERTS_CFG_CHANGED	6	Информация (info)	Изменение конфигурации настройки отзыва сертификатов
0x0068	HEVENT_OCPS_URL_ERROR	3	Ошибка (error)	Проверьте OCSP URL
0x0069	HEVENT_OCSP_RESPONSE_VERIFICATION	3	Ошибка (error)	Ошибка верификации OCSP ответа

Код события	Мнемоника	Уровень критичности		Описание
0x006A	HEVENT_OCSP_RESPONDER_QUERY_FAILED	3	Ошибка (error)	Ошибка отправки OCSP запроса
0x006B	HEVENT_OCSP_CERT_UNKNOWN	3	Ошибка (error)	Неизвестный сертификат – информация о выдаче отсутствует
0x006C	HEVENT_CDP_ERROR	3	Ошибка (error)	Ошибка CDP
0x006D	HEVENT_ERR_INTERNAL	3	Ошибка (error)	Внутренняя ошибка OpenSSL
0x006F	HEVENT_NUMA_ARCE_START	5	Уведомление (notice)	Запуск модуля доверенной загрузки
0x0070	HEVENT_RESET_BIOS_TO_MII	0	Ошибка системы (emergency)	Сброс настроек БСВВ
0x0071	HEVENT_HW_MONITOR_FAIL	3	Ошибка (error)	Нарушена целостность оборудования
0x0076	HEVENT_PASSWD_GUESSING	1	Тревога (alert)	Подбор пароля
0x007C	HEVENT_BIOS_UPDATE	6	информация (info)	Обновление БСВВ с USB-носителя
0x0083	HEVENT_CRL_REFRESH_START	6	Информация (info)	Запуск процедуры обновления CRL
0x0084	HEVENT_CRL_REFRESH_RESULT	6/3	Информация (info) Ошибка (error)	Результат обновления CRL
0x008A	HEVENT_HW_MONITORING	6	информация (info)	Включен контроль оборудования

Код события	Мнемоника	Уровень критичности		Описание
	_ON			
0x008B	HEVENT_HW_MONITORING_OFF	6	информация (info)	Контроль оборудования отключена
0x0091	HEVENT_USER_BLOCKED	3	Ошибка (error)	Пользователь был заблокирован, заносится в журнал при блокировании пользователя
0x00A1	HEVENT_CANT_VERIFY_USER_WITH_PKEY	3	Ошибка (error)	Закрытый ключ, находящийся на токене, не соответствует открытому ключу из сертификата пользователя
0x00A2	HEVENT_ERR_RUTOKEN_SUPPORT_ERR	3	Ошибка (error)	Токен аппаратно не поддерживает заданный алгоритм шифрования
0x00A6	HEVENT_LOAD_TLS_CLIENT_CERT	6	информация (info)	Добавлен клиентский сертификат TLS
0x00AA	HEVENT_PASSWORD_POLICY_CHANGED	5	уведомление	Изменение параметра парольной политики
0x00AB	HEVENT_LOAD_HTTP_BOOT_CERT	6	Информация (info)	Загрузка доверенного сертификата для проверки целостности образа загружаемого по HTTP Boot
0x00AC	HEVENT_HTTP_BOOT_ALLOW_INSECURE	6	Информация (info)	Изменение настроек HTTP Boot: изменение настройки протокола HTTP
0x00AD	HEVENT_WINDOWS_REGISTRY_CONTROL_FAIL	3	Ошибка (error)	Нарушена целостность реестра Windows
0x00AE	HEVENT_WINDOWS_REGISTRY_CONTROL_CHANGE	6/3	Информация (info) Ошибка (error)	Изменение списка контроля целостности для реестра Windows

Код события	Мнемоника	Уровень критичности		Описание
0x00AF	HEVENT_SECURITY_MANAGER_MENU_ENTER	7	Отладочная (debug)	Вход в меню 'Параметры безопасности'
0x00B0	HEVENT_SECURITY_MANAGER_MENU_EXIT	7	Отладочная (debug)	Выход из меню 'Параметры безопасности'
0x00B1	HEVENT_EXT4_JOURNAL_RECOVERY_CHANGED	6/3	Информация (info) Ошибка (error)	Параметры безопасности: изменен параметр контроль транзакций Ext4
0x00B2	HEVENT_NTFS_LOGFILE_CHECK_CHANGED	6/3	Информация (info) Ошибка (error)	Параметры безопасности: изменен параметр контроль транзакций NTFS
0x00B3	HEVENT_FS_TRANSACTION_JOURNAL_NOT_EMPTY	3	Ошибка (error)	Журнал транзакций ФС не пуст
0x00B4	HEVENT_HISTORY_UNLOADED	5	уведомление	Выгрузка журнала аудита на USB, заносится при выборе пункта меню, осуществляющего сохранение информации журнала на USB
0x00B5	HEVENT_HISTORY_DELETED	5	уведомление	Очистка журнала аудита

ПРИЛОЖЕНИЕ 4

СПИСОК СОВМЕСТИМЫХ PCIE УСТРОЙСТВ

В качестве совместимых PCIe устройств могут выступать SATA-контроллер, сетевые устройства.

ПРИЛОЖЕНИЕ 5

ИНСТРУКЦИЯ ПО ГЕНЕРАЦИИ КЛЮЧЕЙ И СЕРТИФИКАТОВ В ОС ASTRA LINUX ВЕРСИИ 1.6 И ВЫШЕ ДЛЯ РАБОТЫ С ТЕХНОЛОГИЕЙ HTTP BOOT

Данный раздел описывает основные настройки для построения инфраструктуры открытых ключей (PKI) с помощью библиотеки OpenSSL в ОС Astra Linux версии 1.6 и выше для работы с технологией HTTP Boot.

1. Предварительная подготовка АРМ с ОС Astra Linux версии 1.6 и выше

Для работ по генерации ключей и сертификатов в ОС Astra Linux необходимо:

– установить пакет библиотек libgost-astra;

– настроить конфигурационный файл;

– создать инфраструктуру УЦ для генерации ключей и сертификатов.

1.1. Установка и настройка пакета библиотек libgost-astra

В состав дистрибутива ОС Astar Linux версии 1.6 и выше (далее - ОС Astra Linux) входит пакет библиотек libgost-astra для выполнения защитного преобразования по алгоритмам ГОСТ.

Для установки данного пакета необходимо:

– вставить установочный диск для ОС Astra Linux версии 1.6 и выше в дисковод;

– авторизоваться под административным пользователем;

– выполнить команду для установки пакета библиотек;

```
apt install libgost-astra
```

– или выполнить установку с помощью графического менеджера пакетов Synaptic (менеджер пакетов устанавливается автоматически при установке ОС и доступен через меню «Пуск» → «Панель управления» → «Программы» → «Менеджер пакетов Synaptic»):

– найти пакет libgost-astra;

– поставить метку "установить";

– нажать кнопку "Применить";

– следовать подсказкам установщика.

Установленный пакет libgost-astra обеспечивает включение в состав методов защитного преобразования, поддерживаемых пакетами OpenSSL, следующих алгоритмов:

– ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 - алгоритмы цифровой подписи;

– поддерживается обмен ключами, основанный на открытых ключах (см. RFC 4357).

Алгоритмы используют

– Закрытые ключи 256 бит для ГОСТ Р 34.11-2001, и 256/512 бит для ГОСТ Р 34.11-2012;

– Открытые ключи 512 бит для ГОСТ Р 34.11-2001 и 512/1024 для ГОСТ Р 34.11-2012;

– ГОСТ Р 34.11-94 алгоритм хеширования. Хэш 256 бит;

– ГОСТ Р 34.11-2012 алгоритм хеширования. Хэш 256 и 512 бит;

– ГОСТ 28147-89 - Симметричное защитное преобразование с ключом 256 бит; Реализованы режимы CBC, CFB и CNT, поддерживается алгоритмы "key meshing" (см. RFC 4357);

– ГОСТ 28147-89 в режиме выработки имитовставки. Базируется на алгоритме симметричного защитного преобразования. Симметричный ключ 256 бит и разрядность вставки от 8 до 64 бит (по умолчанию 32 бит).

– ГОСТ Р 34.13–2015 - Симметричное защитное преобразование «Кузнечик».

1.2. Настройка файла конфигурации с поддержкой ГОСТ алгоритмов

1.2.1. Автоматическая настройка конфигурационного файла

При установке пакета библиотек OpenSSL образец стандартного конфигурационного файла копируется в архив с образцом конфигурации, расположенным */usr/share/doc/libgost-astra/openssl.cnf.gz*.

Для распаковки архива в файл конфигурации */etc/ssl/openssl.cnf* необходимо выполнить команду:

```
gunzip -c /usr/share/doc/libgost-astra/openssl.cnf.gz |
sudo tee /etc/ssl/openssl.cnf > /dev/null
```

Примечание. *Конфигурационный файл заменит существующий (в случае если он был), все внесенные изменения будут уничтожены.*

1.2.2. Ручная настройка конфигурационного файла

Для ручного изменения конфигурации после установки пакета libgost-astra в конфигурационном файле OpenSSL (*/etc/ssl/openssl.cnf*) необходимо выполнить следующие действия:

– добавить в начало конфигурационного файла */etc/ssl/openssl.cnf* строку

```
openssl_conf = openssl_def
```

– в конец конфигурационного файла добавить строки:

```
[openssl_def]
engines = engine_section


[engine_section]
gost-astra = gost_section


[gost_section]
engine_id = gost-astra
dynamic_path = /usr/lib/x86_64-linux-gnu/engines-1.1/gost-
astra.so
default_algorithms = ALL
CRYPT_PARAMS = id-Gost28147-89-CryptoPro-A-ParamSet
```

1.3. Дополнительные изменения в конфигурационный файл

В конфигурационном файле */etc/ssl/openssl.cnf* в разделе [CA_default] необходимо изменить значение директивы "*dir = ./demoCA" на "dir = ./*".

```
[ CA_default ]
dir = ./
```

В дальнейших настройках данный каталог будет использоваться по умолчанию.

В примере будут использоваться расширения для генерации сертификатов. Необходимо убедиться, что расширения включены в стандартном конфигурационном файле, для этого необходимо убедиться, что в конфигурационном файле */etc/ssl/openssl.cnf* имеются записи вида (строки должны быть раскомментированы, т.е. должны отсутствовать

любые знаки типа «#» до начала строки):

```
[ usr_cert ]
# Эти расширения будут добавлены при подписывании запроса на
шим УЦ
basicConstraints=critical,CA:false
keyUsage = nonRepudiation, digitalSignature, keyAgreement
nsComment = "OpenSSL Generated Certificate"
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer

[ v3_ca ]
# Расширения для типового УЦ
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer
basicConstraints = critical,CA:true
keyUsage = cRLSign, keyCertSign
```

Для работы с шаблоном для списка аннулированных сертификатов формата CRL V2 необходимо убедиться, что в конфигурационном файле */etc/ssl/openssl.cnf* имеется строка (строка должна быть раскомментирована, т.е. должны отсутствовать любые знаки типа «#» до начала строки) вида:

```
crl_extensions = crl_ext
```

2. Создание удостоверяющих центров для генерации и работы с сертификатами

2.1. Создание однорангового удостоверяющего центра

Для создания однорангового удостоверяющего центра (далее - УЦ) необходимо осуществить следующие действия:

- создать ключ УЦ;
- создать сертификат УЦ;
- создать ключ клиента;
- создать запрос на сертификат администратора;
- выпустить сертификат для администратора на основе запроса;
- создать списка отзыва сертификатов.

11) Создаем каталог (CA) для удостоверяющего центра, устанавливаем безопасные права доступа. Задаем значение параметра «umask» таким образом, чтобы вновь создаваемые файлы имели права доступа чтения и записи только для создавшего их пользователя:

```
mkdir CA
chmod u=rwx,g=,o= CA
cd CA
umask 066
```

12) Создаем структуру каталогов и файлов для УЦ:

```
mkdir certs crl newcerts private
chmod 700 private
touch index.txt
touch index.txt.attr
echo 1000 > serial
```

Примечание. *Файлы index.txt и serial необходимы, чтобы отслеживать статус выпущенных закрытых ключей и сертификатов.*

13) Создаем закрытый ключ (*private/rootca.key*) для УЦ. В качестве алгоритма для закрытого ключа используется алгоритм ГОСТ Р 34.10-2012 с длиной ключа 256 бит:

```
openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:A
-out private/rootca.key
```

Внимание! Закрытый ключ корневого сертификата удостоверяющего центра является наиболее секретным элементом инфраструктуры открытых ключей и должен быть надежно защищен.

14) Изменяем права доступа к файлу «только на чтение» для пользователя, который сгенерировал данный ключ:

```
chmod 400 private/rootca.key
```

15) Выпускаем корневой сертификат УЦ (*certs/rootca.crt*) (далее CA сертификат), который подписывается закрытым ключом private/*rootca.key*. Для закрытого ключа в сертификате используется алгоритм ГОСТ Р 34.10-2012 с длиной ключа 256 бит.

```
openssl req -new -x509 -md_gost12_256 -days 365 -extensions
v3_ca -key private/rootca.key -out certs/rootca.crt \
-subj /C=RU/ST=SPb/L=SPb/O=ExampleInc/OU=ITdept/CN=ca-server
```

Примечание. *Параметр -days установлен на 365, что означает, что сертификат действителен в течение следующих 365 дней. Для изменения срока действия сертификата необходимо заменить числовое значение 365 на необходимое.*

Корневой сертификат является сертификатом самого удостоверяющего центра и используется для подписи и удостоверения подлинности других сертификатов. Является самоподписанным.

16) Изменяем права на данный CA сертификат:

```
chmod 444 certs/rootca.crt
```

17) Просмотреть содержимое CA сертификата можно командой:

```
openssl x509 -in certs/rootca.crt -noout -text
```

18) Генерируем закрытый ключ для сертификата администратора безопасности (*private/admin.key*):

```
openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:A
-out private/admin.key
```

19) Просмотреть содержимое закрытого ключа можно командой:

```
openssl pkey -in private/admin.key -text
```

20) Для закрытого ключа изменяем права:

```
chmod 400 private/admin.key
```

21) Генерируем запрос на выдачу сертификата в УЦ с использованием закрытого ключа администратора безопасности (`private/admin.key`):

```
openssl req -md_gost12_256 –new –key private/admin.key -out
certs/admin.csr -subj
/C=RU/ST=SPb/L=SPb/O=ExampleInc/OU=ITdept/CN=admin_crt
```

22) Данный запрос на выдачу сертификата подписывается на УЦ:

```
openssl ca -extensions usr_cert -notext -md md_gost12_256 –
keyfile private/rootca.key -cert certs/rootca.crt -in
certs/admin.csr -out certs/admin.crt
```

23) После выполнения команды из п.12 выводится информация о сертификате, производится уточнение о выпуске и подписи данного сертификата. Для завершения процедуры нажмите клавишу «y»:

```
Certificate is to be certified until Jul 29 08:18:30 2021
GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

24) Изменяем права на сертификат:

```
chmod 444 certs/admin.crt
```

25) Создаем файл *crlnumber*

```
echo 1000 > crlnumber
```

26) Создаем список отозванных сертификатов (далее - CRL) с помощью команды

```
openssl ca –keyfile private/rootca.key -cert
certs/rootca.crt  -gencrl -out crl/rootca.crl
```

27) Посмотреть результат можно следующим образом:

```
openssl crl –in crl/rootca.crl -text
```

3. Электронная подпись файла

С помощью OpenSSL возможно создание открепленной (отсоединенной) электронной подписи (далее – ЭП). С помощью открепленной ЭП возможна подпись файла любого формата, при этом сама ЭП записывается в отдельный файл (**.sign*). Для создания ЭП используется закрытый ключ сертификата администратора безопасности (*private/admin.key*), генерируемого в предыдущем разделе.

3.1. Подпись файла и создание ЭП

28) Выбрать файл образ загружаемой ОС, который необходимо подписать для констатации его целостности и подлинности - например, *test.iso*. Подписываем файл образ с помощью закрытого ключа сертификата администратора безопасности *private/admin.key*. Для создания файла ЭП *test.iso.sign* используется алгоритм ГОСТ Р 34.10-2012 с длиной ключа 256 бит.

```
openssl dgst -md_gost12_256  -sign private/admin.key –out
test.iso.sign test.iso
```

Примечание. *Имя файла подписи должно быть идентично имени файла загружаемого образа ОС. Если файл образа загружаемой ОС имеет наименование Filname.iso то файла подписи должен иметь имя Filename.iso.sign.*

3.2. Настройка загрузки в Numa BIOS

Для настройки загрузки с использованием технологии HTTP Boot необходимо:

– создать профиль загрузки, в качестве типа загрузки выбрать «HTTP Boot» (см. п.5.7.2);

– в поле "URL" указать адрес загружаемой подписанной ОС (*test.iso*). Если порт отличается от стандартных (http – 80, https – 443), необходимо указать порт через двоеточие;

– в раздел «Сертификаты» загрузить корневой сертификат УЦ == *certs/rootca.crt*, выработанного в п.2 настоящего приложения;

– в появившемся разделе «Сертификат для HTTP Boot» загрузить сертификат администратора == *certs/admin.crt.*

Данный сертификат также возможно загрузить на сервер, где располагается подписанный образ загружаемой ОС, для этого необходимо переименовать данный сертификат *admin.crt* на *Filename.iso*.crt, где «Filename.iso» имя образа файла загружаемой ОС. Для текущего примера необходимо переименовать файл на *test.iso.sign*;

– загрузить файл ЭП *test.iso.sign* (созданный во время подписи файла *test.iso* в п.3 настоящего приложения) на HTTP(S) сервер, где располагается соответствующий файл образ *test.iso*;

– сохранить профиль загрузки.

ПРИЛОЖЕНИЕ 6

СОЗДАНИЕ И НАСТРОЙКА ПРОФИЛЯ ЗАГРУЗКИ С ОС WINDOWS (ИЛИ ДРУГОЙ ОС) ЧЕРЕЗ USB-НОСИТЕЛЬ В NUMA ARCE

Для создания профиля загрузки необходимо выполнить следующие действия:

1) подключите USB-носитель с образом ОС в СВТ и авторизуйтесь под учетной записью администратора;

2) перейдите в меню «Панель управления» → «Быстрая загрузка» и убедитесь, что подключенный USB-носитель отображается в меню. При отсутствии USB-носителя в списке подключенных носителей просканируйте носители через соответствующий пункт в меню «Быстрая загрузка»;

3) в разделе «EFI-авто» выберите пункт «EFI USB Device»;

4) произведите установку ОС Windows (или иной ОС), следуя указаниям программы-установщика;

5) после установки ОС необходимо создать профиль загрузки. Для этого:

– перезагрузите СВТ и авторизуйтесь под учетной записью администратора;

– перейдите в пункт «Панель управления» → «Конфигуратор» → «Добавить профиль», задайте имя профиля, тип «EFI Hard Drive» и сохраните профиль (см. рисунок 116).

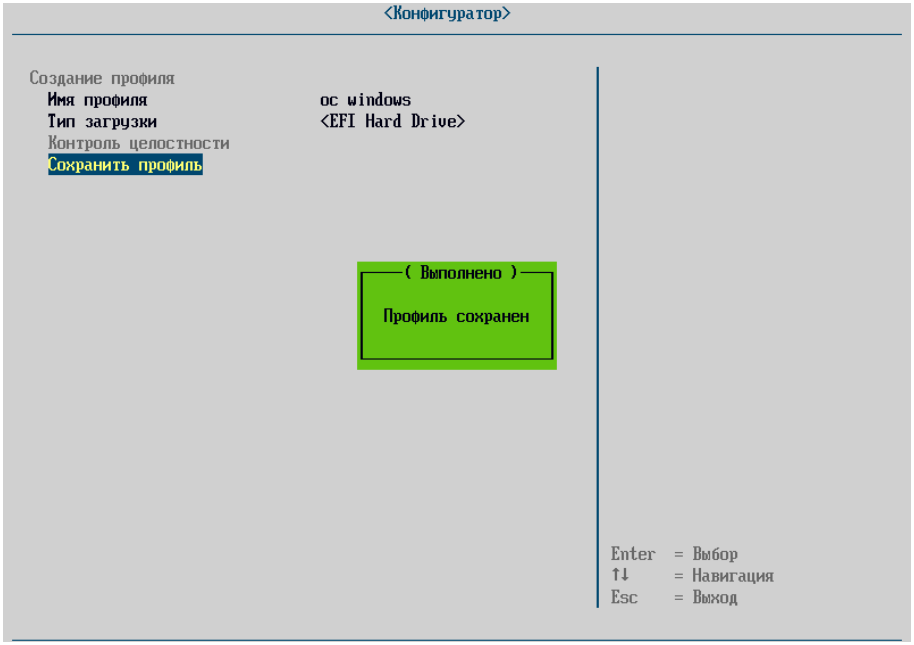

Рисунок 116 – Сохранение профиля загрузки

6) убедитесь, что после сохранения профиля загрузки стал доступен пункт «Контроль целостности»;

7) перейдите в пункт «Контроль целостности» и убедитесь, что загрузочный файл ОС автоматически был поставлен на контроль целостности, и в правом окне отобразилась контрольная сумма файла (см. рисунок 117). Обновите контрольную сумму и сохраните список файлов;

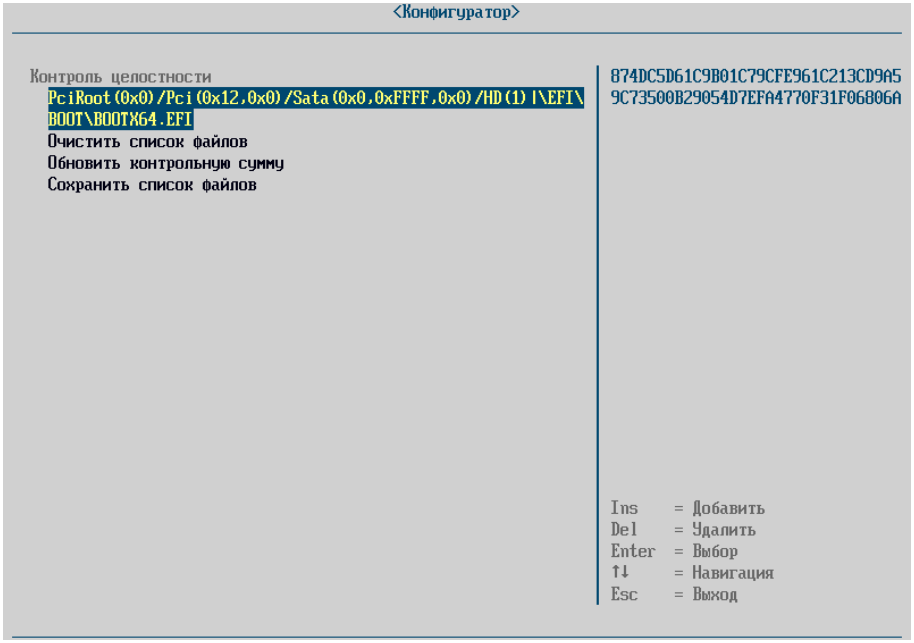

Рисунок 117 – Контроль целостности профиля загрузки

8) перейдите в меню «Панель управления» → «Быстрая загрузка» и убедитесь, что в разделе «Профили загрузки» отображается созданный профиль загрузки.

ПРИЛОЖЕНИЕ 7

ДЕЙСТВИЯ ПРИ НАРУШЕНИИ ЦЕЛОСТНОСТИ ЗАГРУЖАЕМОЙ ОС

1) Убедитесь, что при запуске профиля загрузки на экране появилось сообщение о нарушении целостности модуля ОС (см. рисунок 118) и дождитесь окончания звукового сигнала (звуковой сигнал сработает только при наличии технической возможности СВТ), после чего СВТ произведет перезагрузку;

2) авторизуйтесь под учетной записью администратора, перейдите в меню «Панель управления» → «Проверка целостности» и посмотрите, где произошли изменения, приведшие к изменению контрольной суммы (см. рисунок 119);

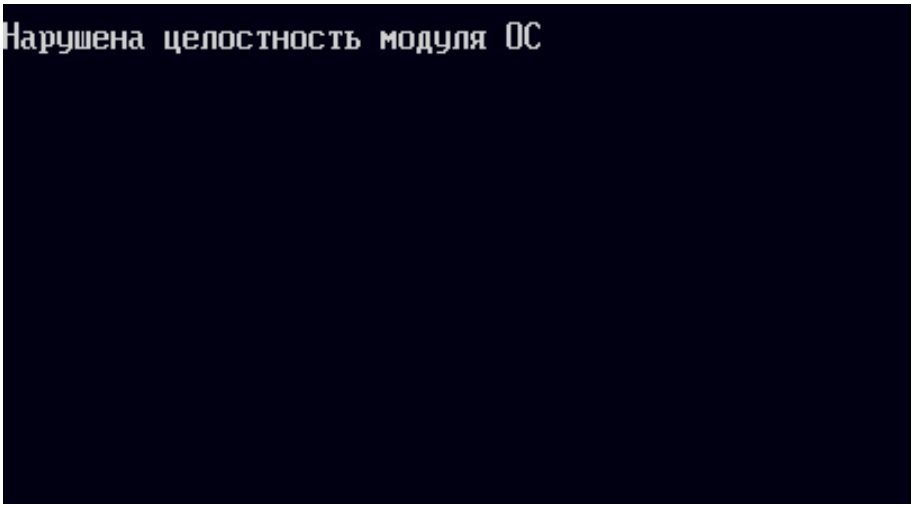

Рисунок 118 – Сообщение о нарушении целостности модуля ОС

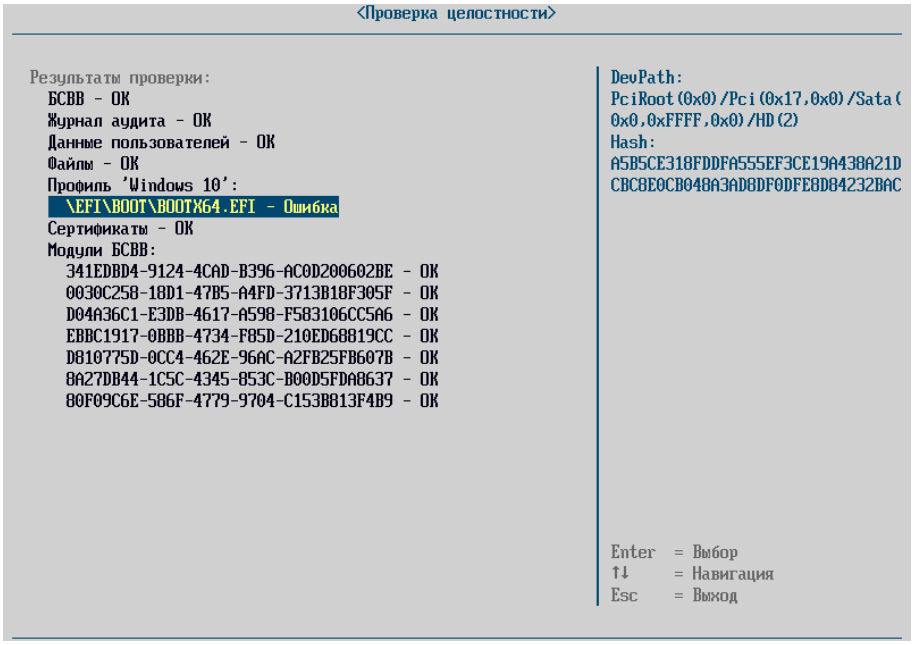

Рисунок 119 – Меню «Проверка целостности»

3) для обновления контрольной суммы файла перейдите в меню «Панель управления» → «Конфигуратор» → <Профиль загрузки, целостность которого нарушена> → «Контроль целостности», обновите контрольную сумму и сохраните список файлов (см. рисунок 120);

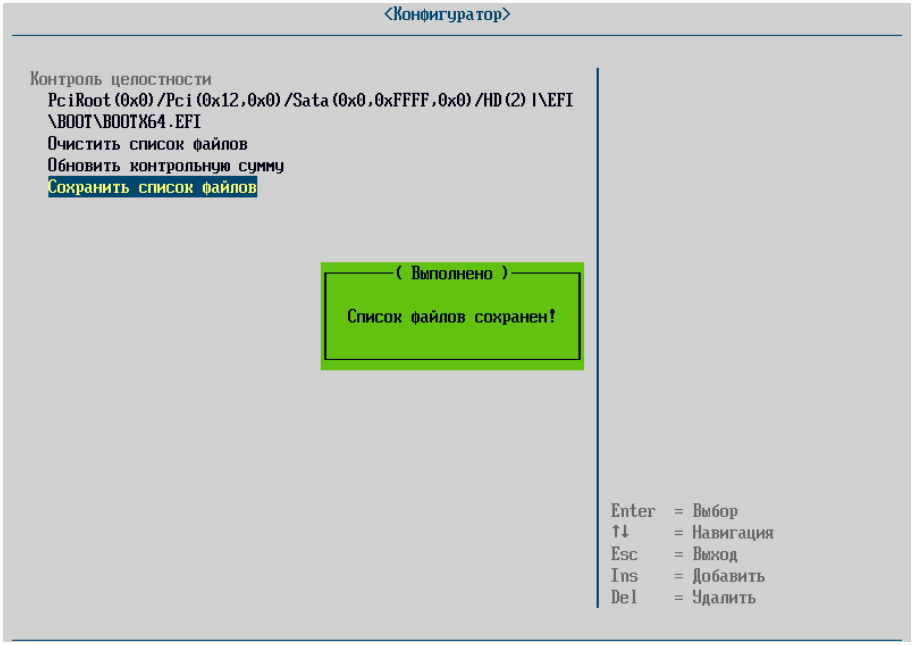

Рисунок 120 – Обновление контрольной суммы

4) запустите профиль загрузки и убедитесь, что контроль целостности успешно пройден;

5) выясните и устраните причину, из-за которой произошла ошибка.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АНП	аутентифицирующий носитель персональный
АРМ	автоматизированное рабочее место
БСВВ	базовая система ввода-вывода
ГОСТ	государственный стандарт
КС	контрольная сумма
МДЗ	модуль доверенной загрузки
НСД	несанкционированный доступ
ОС	операционная система
ПО	программное обеспечение
УЦ	удостоверяющий центр
AHCI	advanced host controller interface
BIOS	basic input/output system
CA	certification authority
CRL	certificate revocation list
DNS	domain name system
FV	firmware volume
GUID	globally unique identifier
IDE	integrated development environment
LDAP	lightweight directory access protocol
PCI	peripheral components interconnect
PIN	personal identification number
TLS	transport layer security
UID	user identificator
URL	uniform resource locator – адрес ресурса
USB	universal serial bus

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ доку- мента	Входящий № сопрово- дительного докум. и дата	Подп.	Дата
	изме- ненных	заме- ненных	новых	аннулиро- ванных					